



ASIC

Australian Securities & Investments Commission

REPORT 11

**Compliance with the Code of
Banking Practice, Building
Society Code of Practice, Credit
Union Code of Practice and EFT
Code of Practice**

April 1999 to March 2000

February 2001

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

February 2001

www.asic.gov.au
ASIC Infoline 1300 300 630

Executive Summary

This report details the results of the annual code monitoring exercise conducted by the Australian Securities and Investments Commission (ASIC). ASIC has responsibility for monitoring industry compliance with the:

- Code of Banking Practice;
- Building Society Code of Practice; and
- Credit Union Code of Practice.

Collectively, these codes are referred to as the payments system codes.

ASIC is also responsible for monitoring compliance with the Electronic Funds Transfer Code of Conduct (the EFT Code).

ASIC inherited responsibility for monitoring the codes from the Australian Payments System Council in July 1998. Monitoring is based on completion of a self-assessment compliance report and dispute statistics by the members of each of the codes.

This report contains information on:

- code membership;
- code compliance;
- compliance assessment;
- staff training;
- arrangements for external dispute resolution; and
- code-related complaints and disputes;

for each of the payments system codes and the EFT Code. It also contains information about implementation of the EFT security guidelines.

The role of the codes

Each of the payments system codes will be affected by the changes proposed under the Financial Services Reform Bill (the FSR Bill). In our view, the codes will remain an important part of the regulatory environment when the FSR Bill has been passed and implemented.

For example, they could serve one or more of three main purposes:

- dealing with consumer protection issues not covered in legislation;
- clarifying what needs to be done to comply with legislative requirements; and/or
- elaborating or building upon legislative requirements.

However, these possible purposes will need further consideration and examination in light of the FSR legislation once passed, and in light of any specific issue addressed.

Independent consultants are currently reviewing the operation of the Code of Banking Practice and the Credit Union Code of Practice. These reviews are likely to address the possible roles for the codes in light of the FSR Bill proposals.

The EFT Code similarly plays an important role in the current regulatory environment, and will continue to do so when the FSR Bill is implemented.

ASIC is currently chairing a working group that is reviewing the EFT Code and expanding the application of the Code so that it is technology neutral. The objective is to ensure that the same protections apply regardless of whether the transaction involves, for example, the use of an ATM, the telephone or the Internet.

ASIC expects to release the revised EFT Code in the first half of 2001.

Code membership

Membership of each of the payments system codes and the EFT Code remains high. To the best of our knowledge, all relevant financial institutions have adopted, or are in the process of adopting, the Code of Banking Practice and the EFT Code of Conduct.

However, we are disappointed that neither the Building Society Code nor the Credit Union Code has full industry coverage. None of the six building societies based in Queensland have chosen to adopt the Building Society Code or another code of similar standards. In addition, there are three credit unions that have chosen not to adopt the Credit Union Code or another code of similar standards. We intend to write to those institutions to encourage adoption of a relevant code.

Code compliance

Most code members reported full compliance with each of the provisions in the respective codes.

There were a small number of institutions that were not able to report full compliance. Of these, some were relatively new market entrants, and still in the process of implementing the codes. Others reported that, once identified, the instances of non-compliance had been remedied or were being corrected.

Compared to the last reporting period, the incidence of reported non-compliance has increased in the case of the Credit Union Code and the EFT Code. However, overall compliance remains high compared to the number of institutions that are members of the various codes.

Compliance assessment

The members of the payments systems codes are required to report on the system of internal assessment used for monitoring compliance with the code and for identifying areas of non-compliance.

All institutions reported that they had established an internal assessment system for monitoring compliance with the code. The type of compliance assessment used did vary between institutions, however, there were some elements (eg appointment of a compliance manager, compliance officer, or compliance unit) that were common to many institutions.

Staff training

Members of the payments system codes and the EFT Code were also asked to provide information on the methods and materials used to train staff about the requirements of the code(s) to which the institution belongs.

Again, the training methods varied between institutions, however, many incorporated some form of training or procedures manual in their programs.

External dispute resolution arrangements

All members of the Banking Code reported that they used the Australian Banking Industry Ombudsman scheme to meet their obligations to provide external dispute resolution process to their customers.

In contrast, credit unions have established a number of different schemes or arrangements for external dispute resolution. The vast majority of credit unions are members of the Credit Union Dispute Resolution Centre, however, a significant number are members of the Credit Union Ombudsman schemes. Other external dispute resolution arrangements are used only by a small number of credit unions.

Members of the Building Society Code have not established an industry-wide external dispute resolution scheme. Instead, they use a combination of small claims and consumer claims tribunals, expert determination and/or a mediation process based on a model developed by the Australian Association of Permanent Building Societies.

Implementation of the EFT Security Guidelines

The former Australian Payments System Council released the EFT Security Guidelines in 1992. They address:

- the positioning of EFT devices where PIN entry is required;
- EFT customer education;
- management of cryptographic keys to protect transactions; and
- communications security.

Information from members of the EFT Code shows that the level of adoption and implementation of the security guidelines remains high.

Complaints and disputes

Between April 1999 and March 2000, banks reported 10,357 disputes under the Code of Banking Practice. This was a significant increase on the number of

disputes in the previous period (8,551). However, the number of transactions made also increased substantially. There was therefore a decrease in the incidence of disputes per million transactions from 2.92 disputes per million transactions in 1998/1999 to 2.72 disputes per million transactions in 1999/2000.

The largest number of disputes under the Banking Code related to the disclosure of fees and charges. Large numbers of disputes were also recorded in relation to PIN based EFT transactions and account crediting and debiting.

In the case of both the Building Society Code, and the Credit Union Code, the largest number of disputes related to PIN based EFT transactions. Disputes about incorrect application of a fee or charge were also high under the Building Society Code, while disputes about disclosure of fees or charges were high under the Credit Union Code.

The number of complaints under the EFT Code has significantly increased. Card issuers reported a total of 106,719 complaints in 1999/2000, compared with a total of 73,125 complaints 1998/1999. This represents an increase from 42 complaints per million transactions in 1998/1999 to 64 complaints per million transactions in the current reporting period.

About two-thirds of the EFT complaints (67,193) in 1999/2000 related to system malfunctions, and most of these were resolved in favour of the consumer.

Twenty-eight per cent of EFT complaints (30,375) involved unauthorised ATM and EFTPOS transactions. Complaints about unauthorised transactions have increased from the previous reporting period overall, however, trends varied between banks, building societies and credit unions.

The majority of these complaints were resolved in favour of the card-issuer; the most common reason being cardholder negligence with their PIN.

The remainder of EFT complaints involved double debit transactions or arose because of confusion over the processing date or merchant name. In previous years, these were recorded as complaints about unauthorised transactions. Most of these complaints were resolved in favour of the card-issuer.

EXECUTIVE SUMMARY	3
INTRODUCTION.....	9
THE ROLE OF THE CODES	10
MONITORING COMPLIANCE	12
ASIC's role	12
The monitoring process	13
Statement of compliance.....	13
EFT Code of Conduct checklist	14
Complaints and disputes.....	14
Implementation assessment – EFT Security Guidelines	15
Proposed review of the monitoring process.....	15
Consistency of the data.....	16
THE CODE OF BANKING PRACTICE.....	17
Scope of the Code.....	17
Methodology	17
Monitoring results	18
Code membership and responses	18
Compliance with the Banking Code	18
Internal compliance assessment.....	20
Staff training	21
External dispute resolution arrangements	21
General comments	21
Complaints and disputes.....	22
THE BUILDING SOCIETY CODE OF PRACTICE	30
Scope of the Code.....	30
Methodology	30
Monitoring results	31
Code membership and responses	31
Compliance with the Building Society Code	32
Internal compliance assessment.....	32
Staff training	33
External dispute resolution arrangements	33
General comments	34

Complaints and disputes.....	34
THE CREDIT UNION CODE OF PRACTICE	38
Scope of the Code.....	38
Methodology	38
Monitoring results.....	39
Code membership and responses	39
Compliance with the Credit Union Code	40
Internal compliance assessment.....	42
Staff training	43
External dispute resolution arrangements	43
General comments.....	44
Complaints and disputes.....	45
ELECTRONIC FUNDS TRANSFER CODE OF CONDUCT.....	53
Scope of the EFT Code.....	53
Methodology	53
Implementing the 1998 amendments to the EFT Code.....	54
Other changes to the monitoring statement.....	54
Monitoring results.....	55
Code membership and responses	55
Compliance with the EFT Code	56
Training methods	61
Implementation of the EFT Security Guidelines	61
Complaints	63
CODE OF BANKING PRACTICE RETURN	71
CODE OF BANKING PRACTICE: STATEMENT OF COMPLIANCE AND DISPUTES STATISTICS.....	71
EFT CODE OF CONDUCT RETURN	77

Section 1

Introduction

Since 1 July 1998, the Australian Securities and Investments Commission (ASIC) has been responsible for monitoring industry compliance with the:

- Code of Banking Practice;
- Building Society Code of Practice; and
- Credit Union Code of Practice.

Collectively, these codes are referred to as the payments system codes.

ASIC is also responsible for monitoring compliance with the Electronic Funds Transfer Code of Conduct (the EFT Code).

The payments system codes and the EFT Code are voluntary, and must be adopted by an institution in order to bind that institution. The codes prescribe certain standards of behaviour and practice for financial institutions in their dealings with consumers. They cover:

- disclosure;
- principles of conduct;
- privacy;
- dispute resolution; and
- in the case of the EFT Code, rules for allocating liability in disputes.

Our first report on compliance with these codes was released in January 2000. This paper, *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*, is on the ASIC website (www.asic.gov.au).

Previously the Australian Payments System Council (APSC) was responsible for monitoring the codes. Compliance results from years before 1999 are in the annual reports of the APSC.

This report gives compliance results for the period April 1999 to March 2000 inclusive.

Section 2

The role of the codes

Before looking at the 1999/2000 results, it is worth providing some brief introductory information about the role of the payments system codes and the EFT Code, particularly in light of the changes proposed under the Financial Services Reform Bill (the FSR Bill). The Code of Banking Practice, the Credit Union Code of Practice, and the Building Society Code of Practice will be the most affected when the proposed legislation comes into effect.

Our recent submission on the review of the Code of Banking Practice stated, among other things, that:

The proposed changes to the financial services market will have a significant impact on banks, as well as other deposit-taking institutions. The role of the Banking Code in this environment needs to be considered.

In our view, the Banking Code could remain an important part of the regulatory environment when the FSR Bill has been passed and implemented. Our present analysis sees codes as serving one or more of three main purposes. They can:

- deal with consumer protection issues not covered in legislation;
- clarify what needs to be done to comply with legislative requirements; and/or
- elaborate or build upon legislative requirements and set out something approaching best (or at least good) practice in an area covered by the legislation.

However, these possible purposes will need further consideration and examination in light of the FSR legislation once passed, and in light of any specific issue addressed.

We also noted that, even though the FSR Bill may make some of the Banking Code's current provisions redundant, the Code should be retained for a number of reasons. For example, the Code:

- addresses matters that are not currently covered by existing or proposed legislation;
- provides a vehicle for addressing emerging consumer issues in a relatively prompt manner;
- provides a mechanism for regularly reviewing and updating bank standards and practices; and
- the monitoring process that is part of the Code provides important feedback to consumers, banks and regulators about the practices and performances of banks.

Our submission on the Credit Union Code of Practice expressed similar views.

Copies of our submissions are on our website (www.asic.gov.au). You can find more information about the reviews of the Code of Banking Practice and the Credit Union Code of Practice at, respectively, <http://www.reviewbankcode.com/index.htm> and <http://www.cu.net.au/codereview/>.

More recently, our Deputy Chair expanded on our views on codes in a speech to the Financial Services Consumer Conference in November 2000.¹ This speech is also available on our website.

The EFT Code similarly plays an important role in the current regulatory environment, and will continue to do so when the FSR Bill is implemented. In particular, it spells out rules for allocating liability in the event of a dispute. No such rules are provided in current or proposed legislation. Without the EFT Code, the normal law of contract would govern these arrangements. These rules could be unfairly weighted against consumers, as was the case before the development of the EFT Code.

ASIC is currently chairing a working group that is looking at expanding the application of the EFT Code. Currently the EFT Code applies only to ATM and EFTPOS transactions. The objective of the ASIC working group is to make the EFT Code technology neutral, to the extent possible, so that the same protections apply regardless of whether the transaction involves, for example, the use of an ATM, the telephone or the Internet.

The group has released two discussion papers,² and expects to release an amended EFT Code in the first half of 2001.

¹ *Monitoring the self-regulatory landscape*, presented by Jillian Segal, Deputy Chair, ASIC to the Financial Services Consumer Conference, 9 November 2000.

² *Second draft expanded EFT Code of Conduct*, ASIC January 2000, and *Discussion paper on an expanded EFT Code of Conduct*, ASIC July 1999.

Section 3

Monitoring compliance

ASIC's role

ASIC has been given a formal monitoring role for each of the payments system codes and the EFT Code. This role is provided for in the codes themselves.

The Code of Banking Practice states that:

The Australian Payments System Council may obtain from the Reserve Bank of Australia consolidated information based on reports and information provided by banks so that the Australian Payments System Council may provide reports to the Treasurer of the Commonwealth on compliance with the Code and its general operation.

The Reserve Bank of Australia will receive each year from each of the banks:

- i. a report on the operation of the Code; and
- ii. information concerning the number of disputes referred to in sections 20.3 and 20.4 of the Code, according to their categories and how each of those categories of disputes has been handled.

Similar provisions are found in the Building Society Code of Practice and the Credit Union Code of Practice.³

Clause 12 of the EFT Code also includes specific reference to a monitoring role for the Commonwealth Government, and an obligation on Code members to annually report on compliance and training.

In exercising this monitoring role, we have adopted an approach similar to that taken by the former APSC: see below.

In addition to our monitoring role, we also have a general responsibility for promoting the adoption of industry standards and codes of practice.⁴ We view industry codes as important tools for consumer protection and market integrity. We will continue to encourage those institutions that have not yet adopted a relevant industry code to adopt, and be fully compliant with, a relevant code.

³ These provisions have not yet been updated to reflect the changes in regulatory responsibilities that came into effect on 1 July 1998. References to the Australian Payments System Council and the Reserve Bank of Australia in the payments system codes should therefore now be read as references to ASIC.

⁴ See section 12FA(1) ASIC Act 1989.

The monitoring process

The current reporting period for compliance with the payments system codes and the EFT Code is 1 April 1999 to 31 March 2000 ("the reporting period"). This is the same period as 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.

The monitoring process primarily involves self-assessment of compliance by code members.

Each institution must complete monitoring statements that together comprise:

- a Code of Conduct checklist or statement of compliance with the relevant code covering the reporting period;
- a report on the number and nature of any disputes that arose during the reporting period; and
- for the EFT Code, an assessment of how the institution has implemented the EFT Security Guidelines.

See Appendix A for a copy of the monitoring statement sent to the members of the Banking Code. A similar statement was sent to credit unions and building societies, reflecting the appropriate code provisions.

See Appendix B for a copy of the monitoring statement sent to EFT Code members.

Monitoring statements were sent to all code subscribers between 30 March and 4 April 2000, with completed returns to be forwarded to ASIC by 12 May.⁵

Statement of compliance

Each member of the Banking, Building Society, and Credit Union Code of Practice has to complete a statement of compliance. The institution's chief executive or other senior officer must sign the statement.

The statement requires institutions to 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 compliance with the Code.

Each institution must also report on:

- whether it has internal assessment systems in place to monitor compliance;
- whether it has identified any recurrent areas of non-compliance;

⁵ As described in Section 7 of this report, CUSCAL collected the completed EFT Code responses of its Redinet affiliate credit unions, and provided a collated and summarised return to ASIC.

- the nature of training provided to staff;
- the name of the external dispute resolution service or process offered to customers; and
- any general concerns about the operation of the Code.

EFT Code of Conduct checklist

In the case of the EFT Code, members must complete an annual Code of Conduct checklist. The checklist is designed to help institutions ensure that they have conformed to all aspects of the Code.

For each provision of the EFT Code, institutions must advise whether or not they have complied with that provision during the reporting period. Institutions must also report on staff training in the Code's provisions.

A letter from a senior executive of the institution must accompany the completed return and checklist:

- certifying that the institution's internal auditors are satisfied that the institution has complied with the Code and, where it has not been able to do so, what is being done to rectify this; and
- including any commentary to qualify or clarify responses.

Complaints and disputes

As well as reporting on compliance, each code member must report to ASIC on:

- the number of code-related disputes that have arisen during the reporting period;
- the categories of disputes; and
- how the disputes were resolved.

Each code contains a specific definition of "dispute". Code members only have to report complaints or disputes that fall inside the relevant definition.

The definition of what constitutes a "dispute" is substantially the same in each of the Banking, Building Society and Credit Union Codes. A dispute arises and must be reported to ASIC when a customer has complained to the institution about a service (and/or product in the case of the Credit Union Code) and is not satisfied with the response given by the institution.

In the case of the EFT Code, members must report on the numbers and types of complaints. The definition of complaints includes *all complaints* about matters falling within the EFT Code of Conduct where the issue of liability arises, or may arise. "Complaints" as defined in the EFT Code is therefore wider than "disputes" (which would include only those EFT complaints that were not immediately settled).

Because the definition of "complaint" in the EFT Code is wider than the definition of "dispute" in the Banking, Building Society and Credit Union Codes, institutions

that are a member of both the EFT Code and one of the Banking, Building Society, or Credit Union Codes will report *all* EFT complaints in their EFT Code report. However, in their return for the Banking, Building Society, or Credit Union Codes, they will only report those EFT complaints that have become disputes.

Finally, each institution must provide information on the number of personal accounts open at the end of the reporting period, and the number of transactions made during this period.

Implementation assessment – EFT Security Guidelines

In the case of the EFT Code, members must also report on how they have implemented the Guidelines for EFT Security ("the Security Guidelines").

The Security Guidelines were released in 1992 by the APSC. They address:

- the positioning of EFT devices where PIN entry is required;
- EFT customer education;
- management of cryptographic keys to protect 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 implementation assessment document devised by the APSC for the original reporting period.

For each of the guidelines, card issuers are asked to report on whether:

- the Guideline has been adopted as policy;
- the Guideline has been incorporated in procedures and processes; and
- further action on the Guideline is proposed.

Proposed review of the monitoring process

As mentioned in our previous report on code compliance, we recognise a need to review the monitoring process to ensure that it is effective and efficient, and does not impose unnecessary burdens on Code members.

In particular, such a review could consider whether:

- the statements of compliance / checklists should be rationalised;
- a new format for the complaint statistics is required;
- the statements of compliance / checklists for the EFT Code and the Banking/Building Society/Credit Union Codes could be merged; and
- some form of complementary external auditing is needed.⁶

⁶ See recommendations 4.1 and 4.2 *Report by the Treasury and the Australian Competition and Consumer Commission on the operation of the EFT Code of Conduct*, March 1998.

We had intended to conduct this review of the monitoring process early in 2000. However, the reviews of the Banking and Credit Union Codes and the EFT Code during 2000 and 2001 may result in changes to those Codes.

The code reviews may also look at whether ASIC or another organisation is the most appropriate body to monitor code compliance. If ASIC does retain responsibility for code monitoring, we would hope to review the monitoring process shortly after the reviews have been completed and any changes to the codes agreed upon. In our submissions to the reviews of payment system codes, we also noted that some form of external monitoring was needed.

Consistency of the data

The information in this report is based on the compliance and complaints data provided by institutions. However, in a small number of cases, institutions provided complaints data that was internally inconsistent.

As can be seen from the monitoring statements in Appendixes A and B, institutions should report total complaints:

- received during the reporting period (A);
- held over from the last reporting period (B);
- resolved in favour of the consumer (C);
- resolved by mutual agreement (D)
- resolved in favour of the issuer (E); and
- outstanding at the end of the reporting period (F).

The total (A + B) should equal the total (C + D + E + F), however, for some institutions this was not the case. However, the inconsistencies were relatively minor and the overall trends discussed in this report still apply.

Section 4

The Code of Banking Practice

Scope of the Code

The Code of Banking Practice ("the Banking Code") was released in 1993 and became fully operational on 1 November 1996. The Banking Code applies to retail transactions in which a bank provides a "banking service"⁷ to a customer. Note that the definition of "customer" means that the Banking Code applies only to personal customers who are dealing exclusively in a private and domestic capacity.⁸

The Banking Code prescribes certain standards of behaviour and practice between the bank and its customers, and covers:

- disclosure of information;
- principles of conduct for general banking requirements; and
- complaints and dispute resolution.

Membership of the Banking Code is voluntary but the Code is binding once adopted.

As noted earlier, the Banking Code is currently under review.⁹

Methodology

The general methodology for monitoring compliance with the Banking Code is described in Section 3 of this report. In summary, Banking Code members are required to complete:

- a statement of compliance with the Code (including information on compliance systems and training); and
- dispute statistics.

⁷ A "banking service" is defined as "a deposit, loan or other banking facility provided by a bank to a customer, but does not include a service in relation to a bill of exchange, a variation of a term or condition of a facility or a debt to a bank that arises as a result of a withdrawal of more than the amount by which an account is in credit without the approval of the bank." (s. 1.1 Banking Code).

⁸ See s. 1.1 Code of Banking Practice.

⁹ See <http://www.reviewbankcode.com/index.htm>.

The statement used to monitor compliance with the Banking Code for the 1999/2000 reporting period was almost identical to the 1998/1999 statement. The only change was to ask each bank to identify the scheme or process it uses for external dispute resolution.¹⁰

Monitoring results

Code membership and responses

At the time of writing this report, there were fourteen Australian owned banks, eleven foreign subsidiary banks, and twenty-five branches of foreign banks operating in Australia.¹¹ However, the Code applies only to banks with retail operations. Nineteen banks operating in Australia at present have significant retail operations and, with one exception, each of these banks has formally adopted the Code. All nineteen banks submitted a monitoring statement for the 1999/2000 reporting period.

The Bank of China has not yet formally adopted the Code. It advised that it is working towards full implementation and noted on its response to the monitoring statement those areas where it is not as yet fully compliant with the Code.

We are very pleased with the high level of adoption of the Code and encouraged by the work of the Bank of China in bringing its procedures into full compliance. We await advice of its formal adoption of the Code.

Institutional mergers have resulted in other changes to the membership of the Code since the previous reporting period. In addition, relatively new entrants AMP Bank and ING Bank implemented the Banking Code during the previous reporting period, and submitted complete returns for this reporting period.

Table 5 shows the membership of the Code of Banking Practice as at 31 March 2000.

Compliance with the Banking Code

In Part 1 of the monitoring statement, banks must report any instances where the bank's internal documentation and procedures failed to comply with the Code.

Two banks reported instances of non-compliance.

The Bank of China is working towards full compliance in the areas of:

- the system of internal assessment for monitoring compliance with the Code;

¹⁰ Under s. 20.4 of the Banking Code, members must have available for their customers an external and impartial process for resolution of disputes that are not resolved satisfactorily by the bank's internal dispute resolution process.

¹¹ See <http://www.apra.gov.au/Societies/ADIs.htm> (downloaded 2/11/00).

- terms and conditions documents for retail deposits; and
- some aspects of staff training.

One other bank advised that it was unable to comply with section 9.3 of the Code in the case of its money market investment product.

For this product, an interest rate change may not be known until the date on which the change takes effect. However, section 9.3 of the Code requires notification (in writing or through advertisements) of such change no later than the day on which the variation takes effect.

ASIC has raised this issue in its submission on the review of the Code.

As well as ensuring that internal documentation and procedures comply with the Code, banks must report on any cases of recurrent non-compliance with the Code.

Banks reported four cases of recurrent non-compliance with the Code during this reporting period: see Table 1 below. In each case, the failure was either rectified or procedures were put in place during the reporting period to rectify the non-compliance.

Table 1 – Recurrent non-compliance with the Banking Code

Instance of non-compliance	Action taken to rectify
During an audit in April 2000 deficiencies were identified in the availability and currency of Code-regulated stationery at a number of Customer Service Centres (CSCs).	Matter raised at the following meeting of district managers. As a result, the current procedures requiring each district manager to conduct random check of the monthly returns submitted by each CSC were reinforced
One business unit had failed to issue the terms and conditions consistently for one of its products during the reporting period. About thirty customers were affected.	Problem was detected during compliance testing and has been addressed.
Recurrent non-compliance in relation to the provision of documents upon new account establishment.	Non-compliance was reported in the Internal Audit Department's report and staff training was initiated to correct the error.
Internal auditing of retail banking section revealed that staff were not aware of the instructions regarding the reporting of customer complaints. Actual customer complaints were handled appropriately, but were not captured or recorded on the standard documentation. Also, documentation supporting the resolution of disputes needed improvement and completed customer feedback reports were often not forwarded to the central support area for collation and analysis	A bank-wide initiative regarding the collection of customer complaints and disputes was undertaken and revised procedures for customer feedback and complaints were implemented.

During the preparation of this report, a consumer organisation raised with us a further instance of non-compliance by a Code member. This involved a failure to provide information about how to cancel a subsidiary card when the bank

approves an application for this card (s. 16.2(ii)). It is not clear whether this practice also occurred during the reporting period.

We approached the bank concerned, and it has amended the relevant standard form letters to include information on how to cancel a subsidiary card.

Internal compliance assessment

Part 2 of the monitoring statement requires banks to report on the system of internal assessment used for monitoring compliance with the Banking Code and identifying areas of non-compliance.

Every bank indicated that management, including senior compliance officers or auditors, has an active role in monitoring compliance with the Code. Each bank also advised that they have established internal assessment systems to monitor compliance with the Code.

These systems include elements or combinations of:

- detailed compliance plans and programs;
- operational procedures and compliance manuals;
- internal auditing; and
- due diligence processes.

Some banks have comprehensive assessment systems that actively identify non-compliance with the Code across all aspects of the bank's business. Other banks use systems that are activated periodically as part of an internal audit program.

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

Here is an example of a compliance system within a bank:

Example

The principal method of assessing compliance with the requirements of the Code is through the monthly due diligence process run by the Group Compliance Manager.

This process monitors possible and actual breaches (if any) of internal policies and procedures relevant to the requirements of the Code as well as the relevant legislation and other codes of practice impacting on the group.

Rectification of compliance issues reported is monitored until they are resolved to the satisfaction of the Group's Executive Risk Committee.

In addition, the Group maintains an internal audit process that includes regular assessment of the Group's operational, procedural and legislative compliance.

The Group's Customer Relations Unit also identifies and reports any instances of non-compliance with the Code and the legislation.

Staff training

All banks advised that they conduct training of staff in the Code, although, as with compliance systems, the methods used varied considerably between individual institutions.

However, some commonly used methods were:

- presentations and seminars;
- induction training;
- videos and on-line training packages;
- self-paced workbooks;
- regular repeat training;
- mentoring systems; and
- group discussions about the implications of the Code to reinforce what has been learnt during training.

Here are some specific examples of training methods..

Example A

The compliance training provided by one bank includes a module on the Banking Code. Examples are given of potential breaches of the Code followed by a discussion of processes to ensure compliance with the Code. The staff also receive a compliance manual for ongoing reference.

Example B

As well as formal training one bank mentioned explicitly that it uses normal internal communication channels, such as internal magazines, bulletins, circulars and regular mentions on the internal television network to reinforce those matters learnt in formal training.

External dispute resolution arrangements

All banks reported that they used the Australian Banking Industry Ombudsman (ABIO) to meet their obligations under section 20.4 of the Banking Code.

Some banks also reported that they used the Financial Industry Complaints Service (FICS), however we presume that this relates to their financial planning arms.

General comments

Four banks commented on the Code.

All four commented about the overlap between the Code and other codes and legislation, and the possibility of inconsistencies arising. The particular regulatory

instruments mentioned were the Uniform Consumer Credit Code (UCCC), the proposed Privacy legislation,¹² and the proposed FSR Bill.

One bank mentioned that the overlap with privacy legislation made it difficult to train staff effectively. Another suggested that the Code should be amended so that the UCCC prevails over the Code. (In fact, clause 1.2 states that the Code is to be read subject to Commonwealth, State or Territory legislation. This would include the UCCC.) A third suggested that the review of the Code should be deferred until the final form of the FSR Bill is known.

In addition to its concerns about possible conflict with other codes and legislation, this third bank raised concerns that:

- the application of the requirement to give 30 days notice of fee variations should not be applicable to "one-off" banking services, eg bank cheques, for which no terms and conditions are issued;
- section 17.1 of the Code (third party guarantors) unnecessarily complicated lending activities, making training and related compliance difficult. The bank is particularly concerned about the need to identify those guarantors referred to in the Code's "related entity" rules.

We have passed copies of these comments to the consultant conducting the review of the Banking Code.

Complaints and disputes

A "dispute" occurs when a customer's complaint about a banking service has been rejected by the bank, and the customer has asked for the decision to be reviewed.

As part of the code monitoring process, banks must give ASIC the statistics on Code-related disputes dealt with internally by the bank.

When a dispute fails to be resolved under a bank's internal dispute resolution processes, it may then be referred to the ABIO. To complement the internal dispute information provided by the banks, we asked the ABIO to provide us with information about disputes resolved externally.

Banks also report on the number of personal accounts open at the end of the reporting period and the number of transactions on these accounts during the period. These statistics allow us to calculate the number of disputes per million transactions.

Not all customers will be satisfied with the result of a bank's internal dispute resolution process. However, we don't know how many of those dissatisfied customers take the next step of referring their dispute to the ABIO, and how many simply let the matter lie. It is important that consumers are aware of all avenues open to them, including their right to approach the ABIO. Individual banks, the ABIO and ASIC can all help to promote the availability of the ABIO to consumers.

¹² The Privacy Amendment (Private Sector) Act was passed in December 2000.

Disputes resolved internally

Table 2 reveals that during the current reporting period, banks reported:

- 10,357 disputes resolved internally;
- 41,055,308 personal accounts open as at 31 March 2000; and
- 3,805,222,878 transactions conducted through those accounts.

This equates to 2.72 disputes per million transactions.

In the previous reporting period from 1 April 1998 to 30 March 1999, banks reported 8551 disputes as against approximately 2.9 billion transactions (2.92 disputes per million transactions).

Table 2 – Trend in Banking Code disputes resolved internally

Year	Number of disputes (incl those held over from 98/99)	Number of accounts	Number of transactions	Disputes per million transactions
1999/2000	10,357	41,055,308	3,805,222,878	2.72
1998/1999	8,551	40,012,410	2,922,670,655	2.92

The overall number of disputes reported is significantly higher than the previous reporting period. However, the total number of transactions made is also significantly higher. The number of disputes per million transactions is therefore lower than the comparable number during the previous reporting period.

In both years the overall number of disputes is significant. Also the narrow definition of "dispute" under the Code may also have a bearing on the number of disputes that are actually recorded and reported to us.

Table 3 shows that of the 10,357 disputes considered internally, the majority of disputes were resolved either in favour of the customer (42.2%) or by mutual agreement (25.1%).

The largest single cause of disputes during the 1999/2000 reporting period was the disclosure of fees and charges (17.5%). Of these disputes, almost half (47.7%) were resolved in favour of the customer, while 21.4% were resolved by mutual agreement and 13.4% were resolved in favour of the bank.¹³

A large number of disputes related to PIN-based EFT transactions (14.4%). These disputes were resolved in favour of the customer and of the bank in almost even proportions (respectively 28% and 26.9%). A smaller percentage (17.6%) were resolved by mutual agreement. A significant percentage of disputes in this category

¹³ This category does not include disputes relating to the existence, application or the level of fees and charges.

(29.3%) were outstanding at the end of the reporting period, indicating perhaps that this type of dispute is more difficult to resolve than others.¹⁴

Account crediting and debiting was another issue that caused a significant number of disputes (13.7%). The majority of these disputes (52.0%) were resolved in favour of the customer, while the remainder were divided in similar proportions between those resolved in favour of the bank, those resolved by mutual agreement, and those outstanding at the end of the reporting period.

A high number of disputes (14.5%) also fell into the "catch-all" category of "Other aspects of service delivery". This includes all other disputes concerning aspects of banking service delivery that are not elsewhere included, and are not a matter of commercial judgment. Banks do not identify the types of dispute included in this category, however, they may include disputes about matters such as fraudulent transactions, incorrect cash given, bank error leading to dishonour or fault in funds transfer, loss of documents, or failure to reply to correspondence.

During the previous reporting period the three categories - fees and charges, EFT and other aspects of service delivery - gave rise to the largest numbers of disputes and the manner of resolution was similar to that in this year's reporting period.

¹⁴ This category includes disputes relating to unauthorised transactions and system malfunction. It excludes complaints that the customer does not pursue further after the initial decision of the institution. However these are reported under the EFT Code.

Table 3 – Banking Code Disputes resolved internally, 1999-2000

Personal Accounts open as at 31 March, 2000: 41,055,308

Transactions Conducted During the Reporting Period: 3,805,222,878

Dispute Category	Total Disputes (incl those held over from 98/99)	Resolution			
		Customer's Favour	Mutual Agreement	Bank's Favour	Disputes Outstanding
Disclosure					
Terms & Conditions	314	120	109	62	27
General Information	353	158	106	50	42
Fees & Charges	1817	866	389	244	324
Cost of Credit	223	101	51	38	36
Foreign Currency Transactions	85	49	24	7	6
<i>Total Disclosure</i>	2792	1294	679	401	435
Variations to Terms & Conditions	130	54	34	18	24
Banking Service Delivery					
Statements	422	270	82	43	24
Account Combination/Closure	247	112	67	47	22
Account Debiting/Crediting	1408	726	281	213	202
Proper Interest Rate, Fee, Charge	687	318	151	141	59
Instructions	706	398	139	93	85
EFT (PIN based)	1490	417	263	401	437
Other Service Delivery	1500	464	718	236	70
<i>Total Banking Service</i>	6460	2705	1701	1174	899
Advertising	26	8	6	9	6
Privacy & Confidentiality					
Disclosure to Related Entities	34	20	11	4	1
Other Aspects of Privacy/Confidentiality	346	121	59	30	63
<i>Total Privacy & Confidentiality</i>	380	141	70	34	64
Provision of Credit	482	134	66	104	183

Guarantees	17	6	6	2	3
Dispute Resolution Process	70	27	36	5	2
Total of All Disputes	10357	4369	2598	1747	1616

Disputes resolved externally

Where disputes are not resolved through the bank's internal process, the consumer can refer them to the Australian Banking Industry Ombudsman.

During the 1999/2000 reporting period, the ABIO reported 2672 disputes about alleged Code breaches (including disputes that had been carried over from the previous reporting period). Just over a quarter of these disputes have been carried over to the forthcoming reporting period.

Again, the total number of disputes reported by the ABIO in this reporting period has increased from the previous reporting period. However, the increase in the number of disputes is also matched by an increase in the number of relevant transactions, and the number of disputes per million transactions (0.70) is only slightly higher than in the previous reporting period (0.64).

Table 4 shows that the largest single number of Code-related disputes referred to the ABIO (733, 27.4%) arose from complaints that the bank concerned had failed to act in accordance with the customer's instructions or authority or on undertakings given to the customer.

As was the case with the banks' internal dispute resolution processes, PIN-based EFT transactions (18.7%), account crediting and debiting (11.1%) and the catchall category "Other aspects of service delivery" (19.6%) together accounted for a significant proportion of disputes referred to the ABIO.

The most common issue in the disputes considered by the banks' internal processes (disclosure of fees and charges) did not figure highly in the matters referred to the ABIO.

The ABIO resolved 2.8% of the disputes reported. Information on the manner of resolution was only recorded in the more complex matters. Of the 37 more complex disputes, just over half (51.3%) were resolved in favour of the customer and 40% were resolved in favour of the bank. In three matters, the result benefited both parties.

Over half of all disputes referred to the ABIO (55.5%) were referred by the ABIO back to the bank, and were resolved at that level. It is pleasing that most disputes are resolved early in the ABIO's processes. However, we would be concerned if the majority of these matters were ones where the bank had an opportunity to resolve the matter before it was referred to the ABIO. If this were the case, it might suggest that the bank's internal dispute resolution processes may not be operating effectively.

In the ABIO's most recent Annual Report, the Banking Ombudsman noted that the internal dispute mechanisms within banks appear to be working with greater effect.¹⁵ We will therefore be interested to see whether statistics change in the next reporting period.

The remainder of disputes reported by the ABIO were discontinued, outside the ABIO's terms of reference, or were outstanding at the end of the reporting period.

During the previous reporting period, the most common areas of dispute also concerned failure to act in accordance with the customer's instructions and PIN-based EFT transactions.

¹⁵ See ABIO Annual Report, 1999-2000, p. 4.

Table 4 – Banking Code Disputes resolved externally, 1999-2000

Personal Accounts open as at 31 March, 2000: 41,055,308

Transactions Conducted During the Reporting Period: 3,805,222,878

Dispute Category	Total Disputes	Resolution							Disputes outside terms of reference	Disputes Outstanding
		Disputes referred back to bank for resolution ¹⁶	Simpler disputes resolved by ABIO ¹⁷	Resolved in Customer's Favour	Resolved by Mutual Agreement	Resolved in Bank's Favour	Discontinued disputes			
Disclosure										
Terms & Conditions	52	23	9	1	0	3	2	1	13	
General Information	69	49	6	0	1	0	1	3	18	
Fees & Charges	104	77	6	0	0	0	5	6	16	
Cost of Credit	18	9	0	0	0	1	0	0	8	
Foreign Currency Transactions	4	2	1	0	0	0	0	0	1	
<i>Total Disclosure</i>	247	160	22	1	1	4	8	10	56	
Variations to Terms & Conditions	41	23	2	0	0	0	1	0	18	
Banking Service Delivery										
Statements	21	11	3	0	0	0	0	0	9	
Account Combination/Closure	23	11	4	0	0	0	1	0	9	
Account Debiting/Crediting	297	182	20	1	0	0	15	7	84	
Proper Interest Rate, Fee, Charge	173	117	15	0	0	0	9	7	41	
Instructions	733	395	57	5	2	4	19	26	251	
EFT (PIN based)	502	232	129	0	0	0	32	1	128	
Other Service Delivery	525	312	45	7	0	3	22	16	142	
<i>Total Banking Service</i>	2274	1260	273	13	2	7	98	57	664	
Advertising	6	4	0	0	0	0	0	0	3	
Privacy & Confidentiality										
Disclosure to Related Entities	7	2	0	0	0	0	2	0	3	
Other Aspects of Privacy/Confidentiality	35	16	1	1	0	1	0	1	17	
<i>Total Privacy & Confidentiality</i>	42	18	1	1	0	1	2	1	20	
Provision of Credit	36	9	6	2	0	3	3	3	15	
Guarantees	21	5	2	2	0	0	1	2	9	
Dispute Resolution Process	5	4	0	0	0	0	0	0	1	
Total of All Disputes	2672	1483	306	19	3	15	113	73	786	

¹⁶ These disputes were referred back to the bank by the ABIO for further consideration. They still met the ABIO criteria for external disputes and are counted as such.

¹⁷ These disputes are simpler disputes resolved by the ABIO – the ABIO does not record whether these disputes were resolved in favour of the customer, the bank or by mutual agreement.

Table 5 – Membership of the Code of Banking Practice

Banks that have adopted the Banking Code of Practice	Banks intending to adopt the Banking Code of Practice
<p>Adelaide Bank Limited</p> <p>AMP Bank Limited</p> <p>Arab Bank (Australia) Limited</p> <p>Australia and New Zealand Banking Group Limited</p> <p>Bank of Western Australia Ltd (Bankwest)</p> <p>Bank of Queensland Limited</p> <p>Bendigo Bank Limited</p> <p>Citibank Limited</p> <p>Colonial State Bank</p> <p>Commonwealth Bank of Australia</p> <p>HSBC Bank Australia Limited</p> <p>ING Mercantile Mutual Bank (Australia) Ltd</p> <p>Macquarie Bank Limited</p> <p>National Australia Bank Limited</p> <p>Primary Industry Bank of Australia Limited</p> <p>St. George Bank Limited</p> <p>Suncorp-Metway Limited</p> <p>Westpac Banking Corporation</p>	<p>Bank of China</p>

Section 5

The Building Society Code of Practice

Scope of the Code

The Building Society Code of Practice ("the Building Society Code") was released in 1994 and became fully operational on 1 November 1996. Similar to the Banking Code, the Building Society Code applies when a building society provides a "service"¹⁸ to a customer.

The Building Society Code prescribes certain standards of behaviour and practice between the building society and its customers and covers:

- disclosure of information;
- principles of conduct in dealings with customers; and
- resolution of disputes.

Membership of the Building Society Code is voluntary but the Code is binding once adopted.

Methodology

The general methodology for monitoring compliance with the Building Society Code is described in Section 3 of this report. In summary, building societies that are members of the Code must complete:

- a statement of compliance with the Code (including information on compliance systems and training); and
- dispute statistics.

The statement used to monitor compliance with the Building Society Code for the 1999/2000 reporting period was almost identical to the 1998/1999 statement. The only change made was to ask the building society to identify the scheme or process used for external dispute resolution.

¹⁸ A "service" is defined as "a deposit, loan or other banking facility provided by the building society to the customer" (s. 1.1 Building Society Code).

Monitoring results

Code membership and responses

There are nineteen building societies operating in Australia,¹⁹ and eleven of these have adopted and implemented the Building Society Code.

During the previous reporting period, the Greater Building Society implemented the Code. It has submitted a complete response for the first time this year and is now fully compliant with the Code.

The IOOF Building Society was previously a member of the Code, but the business was sold on 1 April 1999 and it no longer operates as a building society.

Of the remaining building societies:

- Lifepan Australia Building Society has amalgamated with a credit union. It has therefore adopted the Credit Union Code of Practice and reports in line with that Code.
- Maitland Mutual Building Society has advised us that it intends to adopt the Building Society Code formally and is currently working on bringing its procedures into full compliance with the Code.
- Six building societies in Queensland have not adopted the Building Society Code, nor have they adopted another code of similar scope.²⁰ These are the First Australian Building Society,²¹ Heritage Building Society, Mackay Permanent Building Society, Pioneer Permanent Building Society, The Rock Building Society, and Wide Bay Capricorn Building Society.

It is disappointing that the building societies in Queensland continue to choose not to adopt the Building Society Code. As has been noted in previous monitoring reports, the absence of a code or other formal standards makes it difficult for consumers to assert their rights in the case of a dispute.

In addition, the absence of a code means that there is no guidance on standards for any dispute resolution arrangements. We understand that five of the six building societies are members of the Australian Finance Conference, and therefore participate in the Finance Industry Customer Service dispute handling arrangement established by the AFC. However, this is not a formal dispute resolution scheme, and would not meet the standards required for an ASIC approved dispute resolution scheme.

We will continue to liaise with individual building societies and industry organisations to promote the adoption of the Building Society Code or other codes offering the equivalent level of consumer protection and compliance monitoring.

¹⁹ See <http://www.apra.gov.au/Societies/ADIs.htm> (accessed 2/11/00).

²⁰ They are, however, all members of the EFT Code.

²¹ First Australian Building Society will become subject to the Code of Banking Practice later in 2001 when its merger with a bank is completed.

When implemented, the proposed FSR Bill will ensure that consumers are entitled to certain minimum standards for disclosure of information and dispute resolution even if they belong to a building society that is not a member of the Building Society Code.

Table 8 shows the membership of the Building Society Code and other Codes.

Compliance with the Building Society Code

Monitoring statements were received from all building societies that have adopted the Code.

Part 1 of the statement asks building societies to report on any instances in which the building society's internal documentation and procedures failed to comply with a provision or provisions of the Code. Building societies must also report any cases of recurrent non-compliance with the Code.

None of the building societies reported instances of one-off non-compliance or recurrent non-compliance with the Code during the reporting period.

Internal compliance assessment

In Part 2 of the monitoring statement building societies report on their system of internal compliance assessment.

All building societies advised that they have established internal assessment systems to monitor compliance with the Building Society Code although, as may be expected given the differences in size between building societies, the standard and type of compliance assessment varies between institutions.

Most building societies reported that management, including senior compliance officers or auditors, has an active role in monitoring compliance with the Code. The most common system of compliance assessment reported involves regular or ad hoc auditing by internal audit sections or the internal audit officer.

Some building societies conducted a thorough audit before they adopted the Code and any subsequent change in procedures or documentation is assessed by a legal or compliance officer to ensure compliance with the Code. However, this system does not provide a check on ongoing compliance so is usually supplemented by internal auditing.

Although many building societies are relatively small, some have appointed compliance officers with the specific task of ensuring compliance with the Code. Other smaller building societies reported that supervisory staff or other appropriate staff members share responsibility for compliance with the Code.

The larger institutions often have their own compliance sections for this task.

Here is an example of a compliance system within a building society:

Example

Breaches and complaints are reported to the corporate lawyer at weekly managers' meeting. Every six months the corporate lawyer prepares a report to the due diligence committee which answers to the building society's board. Any instances of non-compliance are dealt with directly by the corporate lawyer and the compliance officer.

Staff training

Building societies were also asked to report on staff training including the methods and materials used to train staff in the Building Society Code and its requirements. All building societies advised that they conduct staff training in the Code, although the extent of ongoing staff training and the methods and materials used varies between individual institutions.

Training methods included:

- training manuals based on standard operating procedures and divided according to the job role of the staff member concerned;
- internal communication by email;
- induction training supplemented by regular training of existing staff;
- training through self-paced workbooks; and
- on the job training.

Here is an example of the training methods used by one building society:

Example

The requirements of the Building Society Code are built into each departmental or sectional procedures manual. During the first two years of employment, employees must progress through a career path that includes testing of knowledge of these manuals. Staff must also be familiar with the legislation and the requirements of the Code as it affects their position.

Satisfactory results must be achieved to move to the next level in the career path.

Ongoing training is conducted for all staff relevant to their branch or department. It is supported by monthly questionnaires distributed to all staff.

Any changes to the Code are notified to the staff training department by the Compliance Officer and then passed on to all the relevant staff.

External dispute resolution arrangements

Unlike banks, building societies do not have an industry-wide external dispute resolution scheme.

Instead, building societies reported that for external dispute resolution, they used a combination of small claims and Consumer Claims Tribunals, expert determination, and/or a mediation process based on a model developed by the Australian Association of Permanent Building Societies (AAPBS). Under the AAPBS model, an external, independent and impartial mediator must be appointed, at the expense of the building society concerned, to hear and resolve the dispute.

It is difficult to properly assess complaints activity and trends, and complaints handling standards, in the absence of an independent external scheme.

General comments

Building societies were asked whether they wished to raise any concerns about the operation of the Building Society Code. However, no comments or concerns were offered.

Complaints and disputes

A "dispute" occurs when a customer's complaint about a service has been rejected by the building society and the customer has asked for the decision to be reviewed by the building society.

Building societies must report information on Code-related disputes dealt with internally by a building society as part of the code monitoring process.

When a dispute fails to be resolved under a building society's internal dispute resolution processes, it may then be referred to the external dispute resolution process. Information on the disputes referred for external resolution is provided directly by the building society concerned.

Building societies also report on the number of personal accounts open at the end of the reporting period and the number of transactions on those accounts during the period. These statistics allow us to calculate the number of disputes per million transactions.

Disputes resolved internally

Table 6 shows that during the current reporting period, building societies reported:

- 168 disputes resolved internally;
- 1,197,706 personal accounts open as at 31 March 2000; and
- 71,806,463 transactions conducted through those accounts.

These figures represent 2.3 disputes per million transactions. There has been an increase in both the total number of disputes, and the number of disputes per million transactions from the previous reporting period. However, the small overall number of disputes makes it difficult to draw any conclusions about the increase.

Table 6 – Trend in Building Society Code disputes resolved internally

Year	Number of disputes (incl those held over from 98/99)	Number of accounts	Number of transactions	Disputes per million transactions
1999/2000	168	1,197,706	71,806,463	2.3
1998/1999	84	973,244	55,430,950	1.5

Table 7 shows that of the 168 disputes considered internally, half were resolved by mutual agreement. The remainder were resolved in favour of the customer or in favour of the building society in approximately equal proportions.

The most common single area for dispute was PIN-based EFT transactions (35 disputes, 20.8%). These were resolved in favour of the building society, in favour of the customer, or by mutual agreement, in approximately equal proportions.

Almost as many disputes (17.7%) were recorded for the incorrect application of an interest rate, fee or charge. Here, the most common resolution was a resolution by mutual agreement. This is consistent with the overall pattern of resolution.

The catchall category – other aspects of service delivery – accounted for 32.1% of disputes. Of these, almost two-thirds (64.8%) were resolved by mutual agreement.

The above results contrast with the results from the previous reporting period, where the most common areas of dispute were:

- disclosure of fees and charges; and
- application of the proper interest rate, fee or charge.

However, given the small number of disputes involved, again it is not possible to draw conclusions as to trends or issues within the industry.

Disputes resolved externally

Where disputes regarding alleged breaches of the Code fail to be resolved internally, they can be referred to an external dispute resolution process. However, during the current reporting period, among all building societies, only one dispute was referred to this process. This dispute involved incorrect application of an interest rate, fee or charge and was resolved in favour of the building society.

Table 7 – Building Society Code Disputes resolved internally, 1999-2000

Personal Accounts open as at 31 March, 2000: 1,197,706

Transactions Conducted During the Reporting Period: 71,806,463

Dispute Category	Total Disputes Received (incl those held over from 98/99)	Resolution			
		Customer's Favour	Mutual Agreement	Building Society's Favour	Disputes Outstanding
Disclosure					
Terms & Conditions	3	0	3	0	0
General Information	14	3	11	0	0
Fees & Charges	7	2	3	2	0
Cost of Credit	5	0	1	4	0
<i>Total Disclosure</i>	29	5	18	6	0
Variations to Terms & Conditions	1	0	0	1	0
Banking Service Delivery					
Statements	2	0	2	0	0
Account Combination/Closure	3	0	2	1	0
Account Debiting/Crediting	8	5	1	1	1
Proper Interest Rate, Fee, Charge	30	10	13	7	0
Instructions	5	1	4	0	0
EFT (PIN based)	35	11	9	14	1
Other Service Delivery	54	13	35	5	1
<i>Total Banking Service</i>	137	40	66	28	3
Advertising	0	0	0	0	0
Privacy & Confidentiality					
Disclosure to Related Entities	0	0	0	0	0
Other Aspects of Privacy/Confidentiality	0	0	0	0	0
<i>Total Privacy & Confidentiality</i>	0	0	0	0	0
Provision of Credit	1	0	0	1	0
Guarantees	0	0	0	0	0
Dispute Resolution Process	0	0	0	0	0
Total of All Disputes	168	45	84	36	3

Table 8 – Membership of the Building Society Code of Practice

Building Societies that have adopted the Building Society Code of Practice	Building Societies intending to adopt the Building Society Code of Practice	Building Societies that report under another payments system code	Building Societies that have not adopted a payments system code
Armidale Building Society Limited	Maitland Mutual Building Society Limited	Lifepan Australia Building Society Limited (Credit Union Code of Practice)	First Australian Building Society ²²
Australian Unity Building Society Limited			Heritage Building Society Limited
Bass & Equitable Building Society Limited			Mackay Permanent Building Society Limited
GIO Building Society Limited			Pioneer Permanent Building Society Limited
Greater Building Society Limited			The Rock Building Society Limited
Home Building Society Limited			Wide Bay Capricorn Building Society Limited
Hume Building Society Limited			
Illawarra Mutual Building Society Limited			
Newcastle Permanent Building Society Limited			
NRMA Building Society Limited			
Territory Mutual Building Society Limited			

²² However, see footnote 22.

Section 6

The Credit Union Code of Practice

Scope of the Code

The Credit Union Code of Practice ("the Credit Union Code") was released in 1994, and became fully effective in 1996. It applies where a credit union provides credit union products or services²³ to a member.

However, the Credit Union Code does not apply to:

- a service involving a bill of exchange;
- an insurance or financial planning service;
- a travel service; or
- the provision of unauthorised credit.

The Credit Union Code contains provisions covering:

- disclosure of information;
- standards of practice; and
- complaints and dispute resolution.

Credit unions adopting the Credit Union Code must incorporate the provisions of the Code into their terms and conditions for members. They must give members a copy of the terms and conditions when or before a credit union product or service is supplied.

Methodology

The general methodology for the monitoring compliance with the Credit Union Code is described in Section 3 of this report. In summary, Code members must complete:

- a statement of compliance with the Code (including information on compliance systems and training); and

²³ A "Credit union product or service" is a deposit, loan or other facility provided by a Credit Union to a member, wholly and exclusively for the member's personal, domestic, or household purposes (s 1.1 Credit Union Code).

- dispute statistics.

As with the Banking and Building Society Codes, the only change made to the 1999/2000 monitoring statement was to ask the institution to identify the scheme or process used for external dispute resolution.

Monitoring results

Code membership and responses

Based on responses to last year's returns, we wrote to the 221 credit unions that we understood were members of the Credit Union Code. We asked each of these institutions to complete the monitoring statement.

Membership of the Credit Union Code changed during the reporting period as a result of some credit unions changing names, merging with others, or ceasing operation. Institutions that had ceased operation after 30 March 2000 were not asked to complete monitoring statements for the 1999/2000 reporting period.

Table 13 shows that, as at 30 March 2000, there were 214 members of the Credit Union Code.

This includes one building society, Lifeplan Australia Building Society, which has amalgamated with a credit union and reports under the Credit Union Code.

It also includes a new credit union, Muslim Community Credit Union, which formed mid-way through the reporting period. This credit union has adopted the Credit Union Code, and will report on compliance in the next reporting period.

To our knowledge, there are only three credit unions that have not adopted the Credit Union Code. They are the Bardon Parish Credit Union, Broadway Credit Union, and Queensland Professional Credit Union. In the last reporting period, the Queensland Professional Credit Union had advised us that it was intending to adopt the Credit Union Code. However, we have since been advised that this credit union is not a member of the Code.

We are very pleased with the high level of adoption of the Credit Union Code. However, we remain disappointed that a small number of credit unions have chosen not to adopt the Code. We intend to write to these credit unions to seek their views and encourage them to adopt this Code or another code of equivalent standard.

We note, however, that many of the Code's requirements may become enshrined in legislation (although not necessarily in the same format) if the proposed FSR legislation is implemented. This legislation would ensure that consumers are entitled to certain minimum standards for information disclosure, staff training, and complaints and dispute handling, even if they belong to a credit union that has not adopted the Credit Union Code.

At the time of preparing this report, all but three current Code subscribers had returned monitoring statements. Those not providing a statement were:

- Newcom Collieries Credit Union;
- Peel Valley Credit Union; and
- Security Credit Union.

After the initial letter sent to all Code members, each of these credit unions was contacted at least three times to remind them to complete and return a monitoring statement.

Compliance with the Credit Union Code

The vast majority of credit unions (96%) reported full compliance with all provisions of the Code (excluding any provisions not applicable).

Nine credit unions reported between them a total of 60 instances of non-compliance with the Credit Union Code during the reporting period. Of these instances:

- 22 instances involved a failure to provide documents and/or information complying with a provision of the Code;
- 14 instances involved a failure to have procedures in place to enable compliance with a provision of the Code; and
- 24 instances involved failure to train appropriate staff in a provision of the Code.

However, for any one clause of the Code, there were no more than three credit unions that reported a negative response.

One credit union reported 30 instances of non-compliance. This credit union advised that:

- terms and conditions for some operational areas had not been updated since the credit union had changed to a new computer system;
- general descriptive information had been allowed to run out of stock; and
- many new staff were not familiar with the provisions of the Code, because training was not held until March/April 2000.

The credit union has taken steps to rectify these matters.

Of the other credit unions reporting one or more instances of non-compliance, two credit unions specifically reported that they had taken steps to correct the non-compliance. We will seek further information from those credit unions that did not provide such a confirmation.

A number of credit unions also reported "not applicable" responses. These primarily involved the Code provisions on payment services, account combination, foreign exchange services, payment instruments, and guarantees. We assume that these "not applicable" responses are because those credit unions provide little or no services in these areas.

During the preparation of this report, instances of non-compliance with both the Credit Union Code and the EFT Code by one credit union were drawn to our attention by a consumer organisation. We have raised these matters with the credit union concerned, and have been advised that it has now taken steps to ensure future compliance (including revising standard form letters, providing additional training, and allocating additional resources to compliance).

Eleven credit unions reported instances of recurrent non-compliance with the provisions of the Credit Union Code. In most cases, credit unions said what they had done to fix the problem. Table 9 gives details of the areas of recurrent non-compliance.

Table 9 – Recurrent non-compliance with the Credit Union Code

Explanation of non-compliance	Steps taken to rectify
Account combinations had occurred incorrectly.	On identifying the problem, the credit union's procedure for account combination was reviewed, and information to members was altered to reflect the new legislative requirements.
Dispute resolution procedure lacked the necessary documentation. Statistical recording of disputes also tends to be lacking.	Over the next few months, the policy on dispute resolution will be updated and distributed to relevant staff members.
Lending checklists identified missing documents.	To be addressed through staff training.
The general information sheet handed out with VISA applications could be confused with the VISA terms and conditions.	Redesigning the relevant documentation solved the problem.
Outdated terms and conditions were available (due to a change in computer system). Also, new staff were not familiar with the Credit Union Code.	Annual training provided. Terms and conditions referred to relevant managers for updating. Stock of general descriptive information reordered.
Some instances of non-compliance identified.	Relevant documentation was corrected or re-written, and procedure training was implemented for staff.
Minor irregularities were identified by APRA at a recent inspection.	Irregularities have now been rectified.
Tax file numbers had not been fully deleted from loan files.	Situation rectified, and tax file numbers are no longer found on documentation.
Point of sale material did not have separate terms and conditions.	Now being urgently rectified.
Some areas of non-compliance in relation to documentation and brochures.	Areas of non-compliance have been actioned immediately to prevent recurrence of errors.
Staff copying documentation from the last copy, or from an old copy of a form.	All out of date documents found in staff personal folders were destroyed. A meeting was held, and the importance of up-to-date documentation was reinforced.

One credit union also advised that it had not yet completed a full compliance review. However, it confirmed that if any areas of non-compliance were identified in the review, corrective action would be taken.

Internal compliance assessment

Credit unions were asked to report on the system of internal assessment used to monitor compliance with the Code provisions and to identify areas of non-compliance.

Credit unions vary considerably in size, with the smallest operating perhaps with one or two part-time staff only. Given the differences in size, we expected that there would be a considerable variation in the scope of the compliance assessment systems used by credit unions. This was found to be the case.

Some of the smaller credit unions do not have a formal compliance assessment system in place. Instead, responsibility for compliance rests with the manager, and staff are trained on the provisions of the Credit Union Code to ensure compliance in the day-to-day conduct of the business.

Most credit unions do have a compliance assessment system in place. However, the scope of the system varies between organisations, and it is not possible to provide a generalised picture. Some features common to a number of credit unions include:

- appointment of a compliance manager, compliance officer, and/or compliance unit, with overall responsibility for compliance with the Credit Union Code;
- establishment of Board subcommittees to oversee compliance;
- use of exception reports that highlight non-compliance;
- use of the compliance manual and compliance notes issued by the Credit Union Services Corporation (CUSCAL);
- random checks of documentation and other procedures;
- formal process for sign-off on documentation changes, which takes into account Code compliance;
- internal and/or external auditing of compliance on a regular basis;
- use of "checklists" to ensure appropriate procedures are followed and relevant documentation provided;
- staff training incorporating Code compliance;
- discussion of compliance issues and procedures at regular staff and/or management meetings.

Here is an example of a compliance system implemented by one credit union:

Example

All staff are given appropriate training from a Code of Practice manual. Department Supervisors check all transactions and new accounts opened as per daily reports and journals. Staff opening new memberships and accounts must complete a Code checklist, and supervisors audit these checklists. In addition, an internal audit is taken to ensure compliance with the EFT Code of Conduct.

Staff training

Credit unions were also asked to provide a brief report on staff training, including methods and materials used to train staff about the Code and its requirements. As with compliance systems, the methods and materials used varied considerably between institutions. However, there were some common themes:

- Many credit unions use external training provided by CUSCAL, as well as the CUSCAL Code compliance manual and CUSCAL bulletins for ongoing reference. Several credit unions also mentioned training material provided by the Credit Union Dispute Resolution Centre.
- Most credit unions include training on the Credit Union Code in the induction program for new staff. Refresher courses on the Credit Union Code are also provided for existing staff at regular intervals (eg every 12 – 18 months).
- Some credit unions provide some form of computer-based training, including interactive software, PC-based modules, CUSCAL CD-ROM, and/or local intranet.
- Many credit unions supplemented formal training with training provided during regular staff training meetings or seminars. These are often provided at weekly or monthly intervals, and, among other things, are used to update staff on any relevant changes.
- Many smaller credit unions also rely on "on the job training". Checklists are popular as an ongoing way to reinforce training about the Code requirements.

Credit unions were asked to identify how training methods varied according to staff function. Many credit unions (particularly the smaller ones) reported that all staff are multi-skilled and trained to the same level. However, other credit unions indicated that training is more specific to an individual's functions and responsibilities.

External dispute resolution arrangements

Currently credit unions use five schemes or arrangements to meet their obligations under section 20.4 of the Credit Union Code. These are:

- Credit Union Dispute Resolution Centre (CUSCAL);
- Credit Union Ombudsman (National Credit Union Association);
- Endispute;
- Dispute Resolution Scheme (managed by a CUSCAL representative in Tasmania); and
- Alternative Dispute Resolution Service, Queensland Department of Justice.

This year, we asked credit unions to identify which alternative dispute resolution (ADR) scheme or process they used. Table 10 lists the results. CUDRC is the most well established scheme and, as expected, it has the largest membership.

Table 10 – Credit union membership of ADR schemes

ADR scheme / process	Number of credit union members
Credit Union Dispute Resolution Centre	167
Credit Union Ombudsman	29
Endispute	6
Tasmanian Dispute Resolution Scheme	2
Alternative Dispute Resolution Service, Qld Department of Justice	1
Total	205

Some credit unions did not identify which ADR scheme they used. However, we examined the list of memberships for the different schemes, and were able to fill in the gaps.

A small number of Code members have not joined one of the schemes:

- Croatian Community Credit Union advised that it intends to join CUDRC;
- Latvian-Australian Credit Co-operative Society advised that it has appointed a well known and respected person from the relevant ethnic community to look at disputes that cannot be resolved internally;
- Manly Vale Credit Union and Westax Credit Society advised that they have established their own schemes or processes for external dispute resolution;
- Lithuanian Co-operative Credit Society Talka advised that it was developing its own process, and that this would incorporate the principles of independence, impartiality, and externality; and
- Although it is a member of the Credit Union Code, Lifeplan Australia Building Society, as a building society, is not eligible for membership of the CUDRC. It advised that it refers unresolved disputes to the Australian Commercial Disputes Centre.

We are concerned about the proliferation of, and variation between, the external dispute resolution processes used by credit unions. The proposed FSR Bill will require all licensed credit union to belong to an external dispute resolution scheme that is approved by ASIC. Criteria for approval are expected to be similar to those in the current ASIC Policy Statement 139, and to be more rigorous than the Code requirements. We are currently discussing with credit union representatives the implications of the proposed legislation for current arrangements.

Asking credit unions to identify their ADR process was a useful exercise and helped us better understand which different ADR processes credit unions use.

General comments

Fifteen credit unions commented on the operation of the Credit Union Code. The main concern raised was the high cost of compliance with the Code, including the

cost of changing documentation. The cost of compliance was a particular concern for smaller credit unions with limited resources.

Others raised concerns that credit union members may neglect to read all the information that is provided to them, and could miss important sections.

One credit union also mentioned the lack of updates flowing through to credit unions on any proposed changes to the Code. It asked for feedback on the results of the monitoring process, or an overview of results from other credit unions highlighting strengths and weaknesses.

We have given a copy of comments relevant to the current review of the Credit Union Code to the taskforce undertaking the review.

We have also noted the concerns about compliance costs, and suggest that they be considered in any review of the monitoring process.

Finally, we will publicise this report and post it on our website (www.asic.gov.au).

Complaints and disputes

Credit unions are asked to provide information on disputes that have been resolved internally. A dispute arises where a credit union's response to a member's complaint is not accepted by that member.

When a dispute fails to be resolved under a credit union's internal dispute resolution processes, it may then be referred to the CUDRC or other external dispute resolution process.

To complement the information from credit unions about disputes resolved internally, we asked each of the various external alternative dispute resolution (ADR) schemes and processes to provide information about disputes referred to them. We received a response from each of those schemes and processes. We also received information about the disputes referred to the four external dispute processes that were established by individual credit unions for use by the establishing credit union only.

Disputes resolved internally

During the reporting period, credit unions reported a total of:

- 1,416 disputes;
- 6,028,662 personal accounts open at 31 March 2000; and
- 463,856,403 transactions conducted during the year.

This equates to 3.1 disputes per million transactions.²⁴

²⁴ The figures for total number of accounts and total number of transactions should be regarded as an estimate only. 21 credit unions could only provide an estimated figure for the number of accounts open and/or the number of transactions made. 19 credit unions did not provide a response to one or both of these questions.

Table 11 shows the types of disputes credit unions recorded during the reporting period. The major area of dispute was EFT (PIN based) transactions (64.1%) and the majority of these disputes (71.2%) were resolved in favour of the customer.

Other significant areas of dispute were:

- disclosure of fees and charges (7.7%); and
- account debiting/crediting (4.7%).

The catchall category – other aspects of service delivery – accounted for 8.3% of disputes.

In the last reporting period, not all credit unions provided statistics on the number of disputes handled internally. It is therefore not possible to compare the *number* of disputes reported during this reporting period with the number of disputes reported during the last reporting period. However, the previous year's figures show that, as with the current reporting period, by far the largest number of disputes resolved internally involved EFT (PIN based) matters (67%).

Table 11 – Credit Union Code Disputes resolved internally, 1999-2000

Personal Accounts open at 31 March, 2000: 6,026,312
 Transactions Conducted During the Year: 463,646,989

Dispute Category	Total Disputes (incl those held over from 98/99)	Resolution			
		Customer's Favour	Mutual Agreement	Credit Union's Favour	Disputes Outstanding
Disclosure					
Terms & Conditions	10	2	3	5	0
General Info	11	3	6	1	1
Fees & Charges	109	28	62	24	2
Cost of Credit	7	2	4	1	0
Foreign Currency Transactions	3	1	0	0	2
<i>Total Disclosure</i>	140	36	75	31	5
Variations to Terms & Conditions	0	0	0	0	0
Banking Service Delivery					
Statements	41	12	26	2	1
Account Combination	17	8	4	5	0
Account Debiting/Crediting	66	34	17	14	6
Proper Interest Rate, Fee, Charge	53	36	13	12	1
Instructions	31	20	8	4	0
EFT (PIN based)	908	646.5	43	179.5	37
Other Service Delivery	117	32	50	24	10
<i>Total Banking Service</i>	1233	788.5	161	240.5	55
	5	4	0	1	0
Advertising					
Privacy & Confidentiality					
Disclosure to Related Entities	3	0	2	1	0
Other Aspects of Privacy/Confidentiality	8	1	2	2	1
<i>Total Privacy & Confidentiality</i>	11	1	4	3	1
Provision of Credit	23	2	8	11	2
Guarantees	0	0	0	0	0
Dispute Resolution Process	4	1	0	2	1
Total of All Disputes	1416	832.5	248	288.5	64

Disputes resolved externally

Table 12 shows the number and type of disputes considered by each of the external ADR processes in Table 10. It also includes the external dispute statistics reported by the four credit unions that have established their own external process.²⁵

The total number of disputes considered by these schemes during the reporting period was 115. This is a substantially smaller number than the previous reporting period, when a total of 767 disputes were reported.

This large difference is primarily due to the fact that, in the previous reporting period, the CUDRC reported to ASIC all of the enquiries and complaints made by consumers. This included all of the initial enquiries that were referred back to the credit union for resolution under their internal dispute resolution process, and were satisfactorily resolved without further CUDRC involvement. This year, the CUDRC has reported only those complaints that have been referred for resolution to the CUDRC, following the failure of the credit union's internal process to resolve the matter.

As with those complaints resolved internally, most disputes involved EFT (PIN based) services. Other common areas of dispute were:

- account crediting/debiting;
- disclosure of fees and charges;
- failure to account in accordance with a customer's instructions; and
- other service delivery (including incorrect cash given, bank error, loss of documents, failure to reply to correspondence, etc).

²⁵ The four credit unions concerned did not refer any matters to their external dispute resolution process during the reporting period.

Table 12 – Credit Union Code disputes resolved externally, 1999-2000

Dispute Category	Total Disputes (incl those held over from 98/99)	Resolution			
		Customer's Favour	Mutual Agreement	Credit Union's Favour	Disputes Outstanding
Disclosure					
Terms & Conditions	11	2	3	2	4
General Info	1	0	1	0	0
Fees & Charges	9	1	3	1	4
Cost of Credit	1	1	0	0	0
Foreign Currency Transactions	0	0	0	0	0
<i>Total Disclosure</i>	22	4	7	3	8
Variations to Terms & Conditions	1	0	0	0	0
Service Delivery					
Statements	5	2	1	1	1
Account Combination/Closure	6	1	3	0	1
Account Debiting/Crediting	9	7	8	2	4
Proper Interest Rate, Fee, Charge	4	1	0	1	2
Instructions	8	0	3	2	1
EFT (PIN based)	35	3	6	8	15
Other Service Delivery	20	2	6	0	8
<i>Total Service Delivery</i>	87	16	27	14	32
Advertising	0	0	0	0	0
Privacy & Confidentiality					
Disclosure to Related Entities	1	0	0	0	1
Other Aspects of Privacy/ Confidentiality	3	1	0	0	0
<i>Total Privacy & Confidentiality</i>	4	1	0	0	1
Provision of Credit	0	0	0	0	0
Guarantees	1	0	0	1	0
Dispute Resolution Process	0	0	0	0	0
Total of All Complaints	115	21	34	18	41

Table 13 – Membership of the Credit Union Code of Practice

Institutions that have adopted the Credit Union Code of Practice			
Access Credit Union (NSW) (formerly Labour Staff Credit Union (NSW))	Central West Credit Union Limited	Education Credit Union Co-operative Limited	Gold Credit Co-operative Limited
ACT Hospitals & Health Employees' Credit Union Co-Operative Limited	CDH Staff Credit Union	ELCOM Credit Union Ltd	Goldfields Credit Union Ltd
Advantage Credit Union Ltd	Cessnock City Council Employees' Credit Union Limited	Electricity Credit Union Ltd	Gosford City Credit Union Ltd
Albury Murray Credit Union Ltd	Circle Credit Co-operative Limited	Encompass Credit Union Limited (formerly Transrail Credit Union)	Goulburn Murray Credit Union Co-operative Limited
Amcor Credit Co-operative Limited	City Coast Credit Union Ltd	Endeavour Credit Union Limited	Grand United Credit Union Limited
AMP Employees' & Agents Credit Union	Coastline Credit Union Limited	Energy Credit Union Ltd	Hardie Employees' Credit Union Ltd
Auburn Municipal Council Employees' Credit Union	Collie Miners' Credit Union Ltd	Ericsson Employees' Credit Co-operative Limited	Health Services Credit Union Society Limited
Australian Credit Union Co-operative	Combined Australian Petroleum Employees' Credit Union Ltd	Esso Employees' Credit Union Ltd	Herald Credit Co-Operative Limited
Australian Central Credit Union Limited	Community First Credit Union Limited	Eurobodalla Credit Union Ltd	Heritage Isle Credit Union Limited (formerly Aluminium Credit Union Co-Operative Society)
Australian Defence Credit Union Ltd	Companion Credit Union Limited	Family First Credit Union Limited (formerly Lithgow Mutual Credit Union)	Hibernian Credit Union Limited
Bananacoast Community Credit Union Ltd	Comtax Credit Union Limited	Fire Brigades Employees' Credit Union Limited	HMC Staff Credit Union Ltd
Bankstown City Credit Union Ltd	Connect Credit Union of Tasmania Limited	Fire Service Credit Union Limited	Holiday Coast Credit Union Ltd
Bemboka Community Credit Union Ltd	Country First Credit Union Ltd	Firefighters Credit Co-operative Limited	Horizon Credit Union Ltd
Berrima District Credit Union Ltd	CPS Credit Union (SA) Ltd	First Gas Employee's Credit Union Limited (formerly AGL Group Employees')	Hoverla Ukrainian Credit Co-operative Limited
BHP Group Employees' Co-operative	CPS Credit Union Co-operative (ACT) Limited	First Pacific Credit Union Limited	Hunter United Employees' Credit Union Limited
Big River Credit Union Ltd	Credit Union Australia Ltd	Fitzroy & Carlton Community Credit Co-Operative Limited	IMG Credit Union Limited
Blue Mountains & Riverlands Community Credit Union	Credit Union Incitec Limited	Flying Horse Credit Union Co-operative Limited	Intech Credit Union Limited
BP Employees' Credit Co-operative	Croatian Community Credit Union Limited	Ford Co-operative Credit Society L Limited	IOOF South Australia Credit Union Limited
BTR Employees' Credit Union	CSR Employees' Credit Union Limited	Gateway Credit Union Ltd (formerly C.B.O.A. Credit Union Ltd)	Island State Credit Union Ltd
B-W Albury Employees' Credit Union Ltd	Dairy Farmers Credit Union Ltd	Geelong & District Credit Co-operative Society Limited	Karpaty Ukrainian Credit Union Limited
Calare Credit Union Ltd	Defence Force Credit Union Limited	Geelong Refinery Club Co-operative Credit Society	La Trobe Country Credit Co-operative Limited
Capral Credit Union Limited	Dependable Credit Union Ltd	GMH (Employees) QWL	La Trobe University Credit Union Co-operative
Capricornia Credit Union Ltd	Discovery Credit Union Ltd		
Carboy (SA) Credit Union	Dnister Ukrainian Co-operative Credit Society		

REPORT 11: Compliance with the Payments System Codes of Practice and the EFT Code of Conduct (April 1999 to March 2000)

Limited	Limited	Credit Co-operative Limited	Limited
Laboratories Credit Union Ltd	Newcom Colliery Employees' Credit Union Ltd	Punchbowl Credit Union Limited	South West Credit Union Co-operative Limited
Latvian Australian Credit Co-operative Society Limited	North East Credit Union Co-operative Limited	Qantas Staff Credit Union Limited	South West Slopes Credit Union Ltd
Lithuanian Co-operative Credit Society (Talka) Limited	North West Country Credit Union Co-operative Limited	Queensland Community Credit Union Limited	Southern Cross Credit Union Limited
Lysaght Credit Union Ltd	Northern Districts Credit Union Ltd	Queensland Country Credit Union Limited	St Mary's Swan Hill Co-operative Credit Society Limited
Macarthur Credit Union Ltd	Northern Inland Credit Union Ltd	Queensland Police Credit Union Limited	St Patrick's Mentone Co-Op Credit Society Limited
Macaulay Community Credit Co-operative Limited	Northern Rivers Credit Union Limited	Queensland Teachers' Credit Union Limited	St Philip's Credit Co-operative Limited
Macquarie Credit Union Ltd	Northern Territory Credit Union Ltd	Queenslanders Credit Union Limited	StateHealth Credit Union Limited
Maitland City Council Employees' Credit Union Ltd	Nova Credit Union Limited	RACV Employees' Credit Union Co-operative Limited	StateWest Credit Society Limited
Maleny & District Community Credit Union Limited	NRMA Employees' Credit Union Ltd	Railways Credit Union Limited	Sutherland Credit Union Limited
Manly Warringah Credit Union Ltd	NSW Teachers Credit Union Limited	Randwick Credit Union Limited	Sutherland Shire Council Employees' Credit Union Ltd
Manning Local Government Employees' Credit Union Ltd	Old Gold Credit Union Co-operative Limited	Reliance Credit Union Ltd	Sydney Credit Union Limited
Maritime Workers of Australia Credit Union Ltd	Orana Credit Union Ltd	Resources Credit Union Limited	TAB Staff & Agents Credit Union Limited
Maroondah Credit Union Ltd	Orange Credit Union Ltd	Rothville Credit Union Limited	Tartan Credit Union Ltd
Media Credit Union Queensland Ltd	Parkes District Credit Union Ltd	RTA Staff Credit Union Limited	Telstra Credit Union Ltd
Melbourne Credit Union Limited	Peel Valley Credit Union Ltd	Satisfac Direct Credit Union Limited	Breweries Union Co-Operative Credit Society Limited
Melbourne University Credit Co-operative Limited	Phoenix (N S W) Credit Union Ltd	Savings & Loans Credit Union (SA) Limited	The Broken Hill Community Credit Union Ltd
Members Australia Credit Union Limited	Plenty Credit Co-Operative Limited	Security Credit Union Ltd	The Credit Union of Canberra Limited
Metropolitan Credit Union Ltd	Point Henry Credit Co-operative Limited	Select Credit Union Ltd	The Gympie Credit Union Ltd
Money Wise Credit Union Limited	Police & Nurses Credit Society Limited	SGE The Service Credit Union Ltd (formerly known as State Government Employees' Credit Union)	The Illawarra Credit Union Limited
MSB Credit Union Ltd (formerly Forestry Commission)	Police Association Credit Co-operative Limited	Shell Employees' Credit Union Limited	The Manly Vale Credit Union Limited
NACOS Credit Union Limited	Police Credit Union Limited	Shoalhaven Paper Mill Employees' Credit Union Ltd	The Police Department Employees' Credit Union Limited
New England Credit Union Ltd	Polish Community Credit Union Ltd	Snowy Mountains Credit Union Ltd	The Scallop Credit Union Co-operative Limited
Newcastle Bus Credit Union Ltd	Post-Tel Credit Union Ltd	Softwoods Credit Union Co-operative Limited	
Newcastle City Council Employees' Credit Union Limited	Power Credit Union Ltd	Sosecure Co-operative Credit Union Limited	
	Powerstate Credit Union Ltd		
	Professionals First Credit Union		
	Prospect Credit Union Ltd		

REPORT 11: Compliance with the Payments System Codes of Practice and the EFT Code of Conduct (April 1999 to March 2000)

Limited	Pulse Credit Union Limited	South East Community Credit Society Ltd	Co-operative Limited
The Summerland Credit Union Limited The TAFE and Community Credit Union Limited The University Credit Society Limited Traditional Credit Union Limited Transcomm Credit Co-operative Limited Transport Industries Credit Union Ltd	Uni Credit Union Limited Unicom Credit Union Limited United Credit Union Limited Upper Hunter Credit Union Ltd Victoria Teachers Credit Union Limited Wagga Mutual Credit Union Ltd	Warwick Credit Union Ltd Waverley Bus Depot Employees' Credit Union Waverley Credit Union Co-operative Limited WAW Credit Union Co-operative Limited Westax Credit Society Ltd Western City Credit Union Ltd	Woolworths/Safeway Employees' Credit Co-operative Limited Wyong Council Credit Union Ltd Yarrawonga Credit Union Co-operative Limited Yennora Credit Union Ltd
Other institutions that have adopted the Credit Union Code of Practice			
Lifeplan Australia Building Society Limited			
Credit unions adopting the Credit Union Code of Practice mid-way through the reporting period			
Muslim Community Credit Union Limited			
Credit unions that have not adopted the Credit Union Code of Practice or another payments system code			
Bardon Parish Credit Union Ltd Broadway Credit Union Ltd Queensland Professional Credit Union Ltd			

Section 7

Electronic Funds Transfer Code of Conduct

Scope of the EFT Code

The Electronic Funds Transfer Code of Conduct (EFT Code) has operated since 1989. It currently covers consumer transactions intended to be initiated through 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.²⁶

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. As well as 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 need for an audit trail.

Card issuers must provide to all cardholders a terms and conditions of use document that outlines the rights and obligations between the parties and includes a warranty that the card issuer will comply with the Code.

Methodology

The general methodology for monitoring compliance with the EFT Code is described in Section 3 of this report. In summary, Code members must complete:

- an EFT Code checklist;
- an Implementation Assessment for the EFT Security Guidelines; and
- complaint statistics.

²⁶ As noted earlier, ASIC is currently chairing a working group to expand the operation of the EFT Code to cover new technologies (see section 2).

The statement used to monitor compliance for the 1999/2000 reporting period is almost identical to the 1998/1999 statement. Minor changes are described below.

Implementing the 1998 amendments to the EFT Code

The EFT Code was last comprehensively reviewed in 1998 by the Australian Competition and Consumer Commission and Treasury. This review resulted in a number of amendments to the text of the Code.

So that we could monitor compliance with these amendments during the 1998/1999 reporting period, the EFT Code checklist was changed. Institutions that had implemented the amendments to the EFT Code were asked to answer additional questions.

As noted in our last report, 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 by April 1999.

For the 1999/2000 reporting period, the changes to the checklist reflecting 1998 amendments to the Code were included as compulsory questions. It was expected that all institutions had made the necessary system and other changes to fully implement these amendments.

Other changes to the monitoring statement

Terms and conditions documents

In previous EFT Code checklists, institutions were asked to provide copies of their terms and conditions (Q. 1). However, there is currently no formal process for reviewing the terms and conditions for compliance with the Code. The request to provide copies has therefore been deleted from the checklist.

Complaint statistics

A number of changes were made to the reporting of complaint statistics in order to implement recommendation 4.2 of the 1998 EFT Code report. These changes were highlighted in bold in the complaints assessment form, and included:

- In section B, the introduction of a new category (*Other*), with subcategories of (a) *confusion over merchant name and/or processing date*, and (b) *double debit transactions*.
- In section C, the deletion of the category 4(a) *Initially reported as unauthorised due to confusion over processing date or merchant name*.

This change meant that complaints about double debit transactions²⁷ were recorded separately for the first time. Previously these complaints were recorded as unauthorised transactions.

In a further change, a new section E dealing with complaints about privacy, was introduced.

As a result of these changes, all complaints will be categorised as:

- system malfunction;
- unauthorised transactions;
- other (confusion over merchant name and/or processing date, and double debit transaction); or
- privacy.²⁸

Other changes to reporting of complaints statistics suggested in the 1998 EFT Code review have not been implemented to date.

Institutions were asked to provide their statistical data in the new complaint categories. However, where an institution's data collection system was not yet amenable to completing the new sections of the complaints data form, institutions were asked to report against the previous format.

Only four institutions advised us that they did not collect complaints statistics in the format required for reporting against some or all of the new categories. They advised that they would be able to report against the new categories in the next reporting period.

Monitoring results

Code membership and responses

There are 56 individual companies that have advised either the former APSC or ASIC that they have subscribed to the EFT Code. The overall number of individual Code members has decreased slightly in this reporting period as a result of institutional mergers and other activity. However, this report also includes information from three institutions (AMP Bank,²⁹ Bank of China, and ING Bank) that have reported under the Code for the first time.

²⁷ A double debit transaction is one where the same transaction is incorrectly debited more than once to the same account.

²⁸ Although, due to the low number of privacy complaints, they have not been included in the following tables.

²⁹ AMP Bank adopted the EFT Code on 12 December 1999, and its return covers the period 12 December 1999 to 31 March 2000.

The majority of individual Code members are financial institutions, and they include banks, building societies, credit unions, finance companies, and charge card issuers. Two companies providing EFT services to financial institutions (First Data Resources and Cashcard) are also members of the EFT Code.

The Credit Union Services Corporation (CUSCAL) subscribes to the EFT Code on behalf of all credit unions affiliated with the Redinet network (155 credit unions). These credit unions are not separately identified as individual Code members. CUSCAL provides us with aggregated statements of compliance, implementation assessments, and dispute statistics from all affiliated credit unions.

Credit unions that are not Redinet affiliates, but have subscribed to the EFT Code are separately identified as Code subscribers.

Table 20 lists all Code subscribers.

To the best of our knowledge, all financial institutions that currently provide retail EFT transactions (as defined by the EFT Code) have subscribed to the Code. This is pleasing as it ensures that all consumers will be governed by the same set of rules, and entitled to an appropriate minimum level of disclosure.

All current Code members completed monitoring statements.

One credit union (Broadway Credit Union) advised that it ceased offering retail EFT services on 1 September 1999. It has therefore provided a return for 1 April – 31 August 1999 only.

Compliance with the EFT Code

There has been a significant increase in the reported instances of non-compliance with the EFT Code in this reporting period. Despite this, the overall level of compliance with the Code remains relatively high.

Excluding CUSCAL/Redinet affiliates,³⁰ 21 Code subscribers reported full compliance with every clause of the EFT Code. Of the remainder, most institutions were compliant with all but one or two of the clauses.

In total, there were 330 instances of non-compliance with Code provisions reported to ASIC. This compares with 33 instances of non-compliance reported in the previous year.

The reasons for this increase are not clear. However, one contributing factor may be delay by some institutions in implementing the 1998 amendments to the Code. Almost one-third of the reports of non-compliance related to Code provisions that were amended in 1998.

It is also possible that in some cases, the reported non-compliance may result from a misunderstanding about the scope and intent of the checklist. For example, institutions that reported a negative response to clause 2.3(iv) may not in fact

³⁰ As CUSCAL provided aggregated responses for its credit union affiliates, it is not possible to identify the number of individual credit unions reporting full compliance.

provide their cardholders with any credit facilities. If this is the case, a "not applicable" response may have been more appropriate.

Of course, not all instances of non-compliance give equal cause for concern. It should also be remembered that the results cover a total of 211 individual institutions (56 individual Code subscribers, and 155 credit unions represented by CUSCAL).

Of those institutions that indicated at least one instance of non-compliance, many provided an explanation and/or indicated that they had taken steps to fix the non-compliance immediately it had been identified.

However, a number of institutions certified that they complied with the Code, despite reporting one or more areas of non-compliance within the checklist, and did not provide advice as to whether the matter had been rectified. We intend to seek further information from these institutions about their plans for rectifying the reported instances of non-compliance.

A disappointing feature of the results is that significant numbers of institutions have not implemented all of the 1998 amendments to the EFT Code. (The amended clauses are identified by # in Table 14.) All institutions were expected to fully implement the changes by April 1999. The results show that many institutions are still lagging in this area. However, a number did provide a timetable by which full implementation of the new requirements will have occurred. We hope that the 2000/2001 monitoring report will show complete implementation of the amendments by all Code subscribers.

Table 14 comments further on specific areas of non-compliance.

Table 14 - Most frequent areas of non-compliance with the provisions of the EFT Code

Clause No (# 1998 Code amendments)	Clause requirement	Subscribers reporting non-compliance ³¹	Additional comments
2.2#	Publish the availability of the institution's terms and conditions.	20	For Redinet affiliates, CUSCAL advises that the terms and conditions detail availability, and documents are also displayed on branch counters.
2.3(ii)	Before EFT card is first used, provide information about the nature of any restrictions imposed by the institution on the use of an EFT card.	5	One respondent noted that information was given verbally.
2.3(ii)	Before EFT card is first used, provide information that merchants and other institutions may impose additional restrictions.	22	All negative responses were from Redinet affiliates. Information is provided in CUSCAL's Visa conditions of use, but not in CUSCAL's Redicard conditions of use.
2.3(iv)	Provide information describing any credit facilities that may be accessed through an electronic terminal.	5	

³¹ These figures include the individual credit union responses provided by CUSCAL.

REPORT 11: Compliance with the Payments System Codes of Practice and the EFT Code of Conduct (April 1999 to March 2000)

3.5#	At the time of advising of an increase in periodic transaction limits, advise that this may increase cardholder liability in the event of unauthorised transactions.	10	One respondent noted that documentation would be fully compliant by August 2000.
------	--	----	--

Table 14 cont.

Clause No (# 1998 Code amendments)	Clause requirement	Subscribers reporting non-compliance	Additional comments
4.1(iv)	On a transaction receipt, provide information about the account being debited or credited.	7	
4.2	Give cardholders the option to receive statements more frequently than 6 monthly.	14	However, a number of respondents indicated that they automatically provided statements on a monthly cycle. ³²
4.2	Advise new cardholders of their options regarding statement frequency.	12	
4.3(i)	Provide on account statements a receipt number or other means to allow cardholders to reconcile the entry with a transaction receipt.	6	
4.3(ii)	Provide on account statements, as a separate item, any charges relating solely to the use of an EFT card and PIN.	11	Some institutions noted that the transaction fees charged are not solely related to EFT usage.
4.4	Include on account statements a suggestion that cardholders should check all entries and promptly notify of apparent errors or possible unauthorised transactions.	33	The majority of negative responses were from Redinet affiliates. CUSCAL advised that the details are set out in conditions of use. Some credit unions promote checking via newsletter. Some do not promote checking regularly on statements.
4.5#	Annually provide a self-contained statement of card and PIN security requirements.	51	For Redinet affiliates, most negative responses indicated that the advice would be given with the next newsletter or bulletin. A number of other institutions advised of expected dates (ranging from June – Oct 2000) when the information would be provided.
11.3	Unless complaint settled immediately, advise cardholders in writing of the procedures for investigation and resolution of complaint.	5	
11.5	Unless complaint settled immediately, or cardholder told of outcome within 21 days, write to cardholders within 21 days to inform them that more time is needed to complete investigation.	7	
11.5	Unless there are exceptional circumstances, complete complaint investigations within 45 days.	10	
11.6	When advising of a decision on a complaint, provide written reasons in terms of the relevant parts of the terms and conditions document.	9	
11.5a#	For investigations continuing beyond 45 days,	7	

³² We take the view that clause 4.2 is not contravened if statements are automatically provided on a monthly cycle.

	provide monthly progress updates.		
--	-----------------------------------	--	--

Table 14 cont.

Clause No (# 1998 Code amendments)	Clause requirement	Subscribers reporting non-compliance	Additional comments
11.5a#	For investigations continuing beyond 45 days, provide a date when a decision can reasonably be expected.	12	
11.10	Where the Code provisions not followed, resolve complaint in cardholder favour.	7	

Training methods

As in previous years, Code members were asked to report on the methods used for training staff on the requirements of the EFT Code.

Institutions reported a variety of training methods. The vast majority (196) had a procedures manual on EFT requirements that was available to all relevant staff. Other frequently used methods included:

- on the job training, both passive (165) and active (168);
- external training (86). This method was particularly used by credit unions, many of whom rely on training provided by CUSCAL;
- special handouts (103); and
- computer based training (83). Again, this method was particularly popular with credit unions.

Implementation of the EFT Security Guidelines

Code subscribers are also asked to report on the implementation of the EFT Security Guidelines, released in 1992 by the APSC.

During this reporting period, institutions were asked to report on three of the four guidelines:

- the positioning of EFT devices where PIN entry is required (eg EFT devices should be designed and constructed to provide for PIN privacy);
- EFT customer education (eg on the potential risks surrounding the use of cards, and on the importance of PIN security); and
- management of cryptographic keys to protect transactions (eg guidelines to ensure that cryptographic keys are generated, transmitted and exchanged in a secure manner).

Table 15 summarises the results.³³

³³ In this table, one response is provided by CUSCAL on behalf of all Redinet affiliates.

Table 15 – Implementation of EFT Security Guidelines, 1999-2000

Responses	Yes	No	Not Applicable
Positioning of EFT devices where PIN entry required			
Adoption of guideline as policy	41	1	15
Incorporation of guideline into procedures, controls and internal audit/assessment processes	41	1	15
Is any further action proposed?	5	38	14
EFT Customer Information			
Adoption of guideline as policy	50	1	6
Incorporation of guideline into procedures, controls and internal audit/assessment processes	51	0	6
Is any further action proposed?	7	44	6
Management of Cryptographic Keys			
Adoption of guideline as policy	51	1	5
Incorporation of guideline into procedures, controls and internal audit/assessment processes	51	1	5
Is any further action proposed?	8	45	4

As this table shows, the level of adoption and implementation of the security guidelines remains high.

One subscriber reported that it had not adopted the guidelines as policy, because it understood "policy" to mean the high level document set down by the subscriber's board. However, it had implemented the guidelines in its procedures, controls, and internal audit/assessment procedures.

A small number of subscribers indicated that they had implemented the guidelines, but their comments showed they had not yet achieved full implementation at the time of reporting.

Two subscribers indicated that they did not consider it necessary to change master keys annually, as is required by the guideline on management of cryptographic keys. This issue may need to be considered if the security guidelines are reviewed.

One subscriber has advised that it had not yet implemented the first guideline as not all parties had been provided with a copy of the guideline. However, it intended to document the guideline for all parties by the end of September 2000.

A number of subscribers reported that one or more of the guidelines were not applicable to their business. Reasons for non-applicability included:

- one subscriber had ceased offering EFT services during the reporting period;
- a number of subscribers do not own or operate ATM or EFTPOS devices themselves; and/or
- some subscribers do not have direct contractual relationships with EFT customers, but provide technical services to financial institutions.

Further action planned by subscribers on one or more of the guidelines included:

- developing/upgrading installation guidelines for third party Point of Sale device installers to include suitable PIN privacy related information;
- updating merchant agreements to include guidelines, and developing merchant instruction booklets by December 2000;
- new inserts or statements for customers regarding security issues;
- replacement of older devices that are not able to meet the guidelines; and
- ongoing reviews.

During 2001, we will examine the need for review of the EFT Security Guidelines.

Complaints

As for the payments system codes, subscribers to the EFT Code must provide information about complaints.³⁴

With one exception, all Code subscribers' returns included the required information on complaints considered under the Code. Diners Club advised that its current data collection system did not allow it to provide complaints information in the manner requested. We have confirmed with Diners Club their obligation to report on complaints data, and noted that they have agreed to make the necessary system changes to ensure that they are able to provide this complaints information next time.

Code subscribers reported approximately 1,650 million EFT transactions in the year to March 2000.³⁵

The number of transactions reported has decreased in comparison with the year to March 1999 (1,710 million). One possible explanation for this change might be that some consumers are switching to technologies not yet covered by the EFT Code

³⁴ The definition of "complaints" in the EFT Code is wider than the definition of "disputes" in the payments system codes: see explanation under "Complaints and disputes" in Section 3 of this report. Thus, the number of EFT disputes reported by institutions under the payments system codes will not necessarily be the same as the number of complaints reported under the EFT Code.

³⁵ At the time of writing this report, one institution had not been able to provide data on the total number of transactions. In addition, three institutions were not able to provide transaction data for the full 12 months of the reporting period. In those cases, the part year figures were averaged so that a 12 month figure could be estimated.

(eg telephone banking and internet banking) for some or all of their electronic banking transactions.

Table 16 shows that 106,719 complaints (excluding privacy complaints) were considered during the reporting period. This figure includes complaints held over from the previous reporting period.

Table 16 – Trend in EFT Code complaints

Year	Number of complaints (incl those held over from 98/99)	Number of transactions	Complaints per million transactions
1999/2000	106,719	1,655,373,445	64
1998/1999	73,125	1,710,904,716	42

The number of complaints has increased significantly since the previous reporting period, even though the number of transactions has decreased slightly.

Table 17 shows that:

- 67,193 complaints related to system malfunction;
- 30,375 complaints related to unauthorised transactions; and
- 9,151 complaints were other complaints (double debits or confusion about merchant name or processing date).

Complaints about system malfunction were generally resolved in favour of the cardholder, while complaints about unauthorised transactions and other complaints were generally resolved in favour of the card-issuer.

Table 17 – EFT Code complaints, 1999-2000

Complaint Type	Total complaints (incl those held over from 98/99)	Resolution			
		Issuer Liable	Customer Liable	Complaints outstanding	Unaccounted for
System Malfunction	67193	47929	15362	3898	4
Unauthorised transaction	30375	11510	15728	3204	-67
Other (confusion over merchant name, double debits)	9151	2193	6988	70	-100
TOTALS	106719	61632	38078	7172	

Table 18 displays this information in complaints per million, and compares it with the previous year's results. This shows that the proportionate incidence of complaints about system malfunctions has almost doubled, increasing from 26 to 41 complaints per million transactions.

Complaints about unauthorised transactions are of greatest concern to consumers and create some of the more difficult issues to resolve. However, comparing the incidence of complaints about unauthorised transactions with the previous year's results is more complicated. This is because the category of unauthorised transactions no longer includes complaints about double debits and complaints resulting from confusion over merchant name or processing date. The types of complaints that will be included in this category have therefore fallen compared to the previous reporting period.

Even so, it is possible to make some assessment of the change. In the previous reporting period, almost one-third (8168) of the complaints about unauthorised transactions were reported initially as unauthorised due to confusion over processing date or merchant name. In this reporting period, these types of complaints have been recorded in a different category.

It is not possible to identify the number of complaints about double debits that were included in the unauthorised transactions category in the previous reporting period, as these types of complaints were not separately identified.

Given the above, there was likely to be no more than 17,295 complaints about "pure" unauthorised transactions (i.e. not including complaints where there was initial confusion about the merchant name or date, or complaints about double debits) in the previous reporting period. Thus, it can be estimated that the number of complaints about "pure" unauthorised transactions has increased by at least 75%.

Similar reasoning suggests that the number of complaints about "pure" unauthorised transactions appears to have increased from no more than 10 complaints per million transactions in 1998/1999 to 18 complaints per million transactions in 1999/2000.

Although these are only estimated figures, they do suggest that the number and incidence of complaints about "pure" unauthorised transactions has increased quite significantly in the current reporting period. It is not clear why there has been such an increase. However, Table 19 shows that complaints to minor banks have shown the greatest increase.

Table 18 – EFT Code complaints (per million transactions) 1999-2000

Complaint Type	Total rec'd (incl those held over from 98/99)	Resolution			Total 98-99
		Issuer Liable	Customer Liable	Outstanding	
System Malfunction	41	29	9	2	(26)
Unauthorised Transactions	18	7	10	2	(16)
Other (confusion over merchant name etc, double debits)	6	1	4	0	(recorded as unauthorised transactions in 98-99s)

To give a more detailed picture of these complaints, Table 19 disaggregates the complaints by institutional grouping (major bank, minor bank, building society, and credit union). We have not included information from non deposit-taking institutions in this table, as the small number of institutions in this group that process transactions distorts the information.

Again, care must be taken in interpreting these figures, as the category of unauthorised transactions used this year is smaller this year compared to the previous year.

Table 19 shows that, compared to the previous reporting period, there has been little change in the number of complaints made to major banks and credit unions about unauthorised transactions. Similarly, the number of complaints made to building societies has increased only slightly, from 14 to 17 complaints per million transactions.

In contrast, the number of complaints made to minor banks has increased dramatically, from 5 complaints per million transactions last year to 20 complaints per million transactions this year. The reasons for this change are not clear.

It is also interesting to note that the minor banks and building societies are much more likely to resolve a dispute about an unauthorised transaction in favour of the card issuer. In contrast, the major banks and the credit unions appear to have a more even distribution of liability.

Table 19 – Unauthorised transaction complaints by major institutional groupings (complaints per million transactions)

Institution	Total rec'd & considered	Resolution			Total 98-99
		Issuer liable	Customer liable	Outstanding	
Banks					
Major	18	8	9	2	(20)
Minor	20	5	15	1	(5)
	14	2	13	0	(17)
Building Societies					
Credit Unions	14	7	5	3	(14)
Total all institutions	18	7	10	2	(16)

Table 20 provides a detailed breakdown of the reasons for cardholder or card-issuer liability in the case of unauthorised transactions reported by all Code subscribers.

In almost half of the cases where the cardholder was considered liable, liability was a result of negligence with the PIN (48.4%). The other common reason for cardholder liability was where the cardholder was liable for only \$50 because it was unclear whether or not they had contributed to the loss (16.0%).

A significant category for cardholder liability last year was where the transaction was initially reported as unauthorised due to confusion over processing date or merchant name. These complaints are no longer recorded in the unauthorised transactions category.

In almost a quarter of cases where the cardholder was found liable, liability was imposed because the investigation was terminated (24.0%). This is a substantial increase from last year, when only 5% of investigations were terminated.

The reason for this increase is not immediately clear. It may be that card issuers recorded complaints due to confusion over merchant name or processing date in this category, instead of in the new category introduced this year. To minimise the chance of this occurring for the next reporting period, we will emphasise the changes to the complaints form when the 2000/2001 statements are distributed. If, despite such a clarification, the anomaly continues in the next reporting period, some other explanation might need to be considered.

For complaints about unauthorised transactions where the card issuer accepted liability, the major reasons for liability were:

- it was clear neither the cardholder nor issuer contributed to the loss (58.0%);

- the matter was settled without formal investigation (23.7%);
- the losses occurred before the cardholder received their card and/or PIN (11.4%).

This result is similar to that for the 1998/1999 reporting period.

This year, we also asked card issuers for information about any complaints that they had received relating to the privacy provisions of the EFT Code. Only one institution (a credit union) reported a privacy complaint. This complaint was resolved to the customer's satisfaction.

Table 20 – Liability for Unauthorised Transactions, 1999-2000

Customer's Liability (for at least part of the loss)	Number of complaints	% of Customer Liabile	Total 98-99
1. Customer Liability limited to \$50 (s.5.5)	2506	16.0%	(675)
2. Customer Negligent with PIN (s.5.6)	7569	48.4%	(7901)
3. Unreasonable delay in notification of loss or theft of card, etc. (s.5.7)	433	2.8%	(169)
4. a. Other	19	0.1%	
b. ATM deposit shortfall	571	3.6%	(171)
c. Investigation terminated	3762	24.0%	(945)
d. Evidence of fraud or other offence	788	5.0%	(240)
Total of all Types of Consumer Liability	15648		
Issuer Liabile	Number of complaints	% of Issuer Liabile	Total 98-99
1. Settled without formal investigation	2652	23.7%	(4241)
2. Breach of Code by Institution (s.11.10)	281	2.5%	(62)
3. Conduct by Employees of Institution			
a) Negligent conduct by employees of institution (s.5.2(I))	46	0.4%	(7)
b) Fraudulent conduct by employees of institution (s.5.2(I))	17	0.2%	(0)
4. Conduct by employees / agents of merchants			
a) Negligent conduct by employees / agents of merchants (s.5.2(I))	90	0.8%	(28)
b) Fraudulent conduct by employees / agents of merchants (s.5.2(I))	159	1.4%	(10)
5. Cards forged, faulty, expired or cancelled (s.5.2(ii))	5	0.0%	(119)
6. Losses occurred before cardholder received card or PIN (s.5.2(iii))	1273	11.4%	(185)
7. Losses occurred after notification of loss or theft of card (s.5.3)	183	1.6%	(257)
8. Losses where it is clear neither the cardholder or issuer contributed to loss (s.5.4)	6504	58.0%	(4750)
Total of All Types of Issuer Liability	11210		

Table 21 – Membership of the EFT Code of Conduct

Institutions that have adopted the EFT Code	
Adelaide Bank	Heritage Building Society Limited
Australian Guarantee Corporation Limited	Home Building Society Ltd
American Express International Inc	HSBC Bank Australia Limited (formerly Hong Kong Bank)
AMP Bank Limited	Hume Building Society Ltd
Australia and New Zealand Banking Group Limited (incorporating Town & Country Bank)	Hunter United Employees' Credit Union Ltd
Armidale Building Society Ltd	Illawarra Mutual Building Society Ltd
Bananacoast Community Credit Union Ltd	ING Bank (Australia) Ltd
Bank of China	Mackay Permanent Building Society Ltd
Bank of New Zealand	Macquarie Bank Limited
Bank of Queensland Limited	Maitland Mutual Building Society Limited
Bank of Western Australia Ltd	National Australia Bank Limited
Bass & Equitable Building Society Ltd	Newcastle Permanent Building Society Ltd
Bendigo Bank	NRMA Building Society
Broadway Credit Union Ltd (ceased membership on 1 September 1999)	Phoenix (NSW) Credit Union Limited
Capricornia Credit Union Ltd	Pioneer Permanent Building Society Ltd
Cashcard Australia Limited	Police Association Credit Co-operative Limited
Citibank Limited	Qantas Staff Credit Union
Coastline Credit Union Ltd	Queensland Country Credit Union Ltd
Coles Myer Ltd	Queensland Police Credit Union Limited
Colonial Ltd	Queensland Professional Credit Union
Colonial Trust Bank	St George Bank Limited
Commonwealth Bank of Australia	Suncorp-Metway Ltd
Credit Union Services Corporation (Australia) Ltd (representing 155 credit union Redinet affiliates)	Territory Mutual Building Society Ltd
Diners Club International	The Rock Building Society Limited
First Australian Building Society Limited	Upper Hunter Credit Union Ltd
First Data Resources (Part B only applicable)	Warwick Credit Union Ltd
GE Capital (incorporating AVCO Access)	Westpac Banking Corporation (incorporating Bank of Melbourne and Challenge Bank)
Greater Building Society Ltd	Wide Bay Capricorn Building Society Ltd
Herald Credit Co-operative Limited	

Appendix A

Code of Banking Practice return

CODE OF BANKING PRACTICE: STATEMENT OF COMPLIANCE AND DISPUTES STATISTICS

INSTITUTION: (please print name) _____

For period: April 1999 - March 2000

CONTACT OFFICER:

Name: _____

Telephone: _____

Position: _____

Address: _____

Facsimile: _____

E-mail: _____

Date: _____

From 1 July 1998, the Australian Securities and Investments Commission has been charged by the Commonwealth Government with monitoring the implementation of, and compliance with, the Code of Banking Practice ("the Code"). Explanatory Notes are attached. 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.

Completed returns are to be forwarded to:

Nicola Howell

Office of Consumer Protection

Australian Securities and Investments Commission

GPO Box 4866

SYDNEY NSW 1042

by 12 May 2000.

Part 1

For each product/service covered by the Code:³⁶

Code of Banking Practice - Relevant Section	Does your institution have DOCUMENTS &/or INFORMATION which comply with the Code in relation to: (Yes/No/NA)		Does your institution have PROCEDURES in place to enable compliance with the Code in relation to: (Yes/No/NA)		Does your institution TRAIN appropriate staff in the requirements of the Code in relation to: (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	

Part C - Resolution of disputes

Dispute resolution (s 20)	19.1		19.2		19.3	
---------------------------	------	--	------	--	------	--

³⁶ 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 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. Please provide the name of the external dispute resolution scheme you use for the purpose of compliance with clause 20.4 of the Code. If you are not a member of an established dispute resolution scheme, please provide summary details of the process used for external dispute resolution.

5. 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/Nominee³⁷.

..... Date:.....

³⁷ Nominee should be an appropriate, senior officer; please indicate position held.

CODE OF BANKING PRACTICE - STATISTICAL RETURN

Period: April 1999 - March 2000

PART A	NUMBER OF DISPUTES	Concerning:	MANNER OF HANDLING DISPUTES "RESOLVED" INTERNALLY						
			Outstanding from prior period	Received during period	In favour of Customer	Mutual Agreement including goodwill decisions	In favour of Bank	Outstanding at end period	
			A	B	C	D	E	F	
		Disclosure:-							
1		Terms & Conditions							
2		General Information							
3		Fees & Charges							
4		Cost of Credit							
5		Foreign Exchange Services							
6		Variation to Terms & Conditions							
		Banking Service Delivery:-							
7		Statements							
8		Account combination/closure							
9		Account debiting/crediting							
10		Proper interest rate, fee or charge							
11		Instructions							
12		EFT (PIN-based)							
13		Other aspects - banking service delivery							
14		Advertising							
		Privacy & Confidentiality:-							
15		Disclosure to Related Entities							
16		Other aspects - privacy/ confidentiality							
17		Provision of Credit							
18		Guarantees							
19		Dispute Resolution Process							

PART B	
DENOMINATOR DATA	
Number of:-	
20 Personal accounts	_____ At end period (March 2000)
21 Personal transactions	_____ During period (April 1999 - March 2000)

Appendix B

EFT Code of Conduct return

ELECTRONIC FUNDS TRANSFER CODE OF CONDUCT MONITORING STATEMENTS

INSTITUTION: (please print name) _____

For period: April 1999 - March 2000

CONTACT OFFICER:

Name: _____

Address: _____

Telephone: _____

Position: _____

Facsimile: _____

Email: _____

Date of completion: _____

From 1 July 1998, the Australian Securities and Investments Commission has been charged by the Commonwealth Government with monitoring the implementation of, and compliance with, the EFT Code of Conduct. In completing the monitoring statements, 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.

The monitoring statements are in three sections:

Part A EFT Code of Conduct checklist

Part B Guidelines for EFT Security, Implementation assessment

Part C Complaint resolution assessment

All three sections must be completed.

You should return to the Australian Securities and Investments Commission the completed monitoring statements, together with a covering letter from a senior executive of your organisation:

- . 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.

Completed returns are to be forwarded to:

Nicola Howell
Office of Consumer Protection
Australian Securities and Investments Commission
GPO Box 4866
SYDNEY NSW 1042

by **12 May 2000**.

PART A

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION
E. F. T.
CODE OF CONDUCT CHECKLIST

PART B

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION
GUIDELINES FOR E.F.T. SECURITY
IMPLEMENTATION ASSESSMENT

PART C

AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION
COMPLAINT RESOLUTION ASSESSMENT

PART A

E. F. T. CODE OF CONDUCT CHECKLIST

This checklist is designed to help institutions ensure that they have conformed with all aspects of the EFT 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:

- . 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.

Yes No

SECTION 1: INFORMATION DISCLOSURE

Terms and Conditions

1. Have you developed Terms and Conditions of Use documents that reflect the requirements of the Code? _____

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) 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? _____

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? _____

	Yes	No
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?		
9(a) 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?	_____	_____

	Yes	No
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?	_____	_____
. 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?	_____	_____

	Yes	No
17. Did you send a statement or record of account activity to cardholders at least every six months?	_____	_____
17(a) 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?	_____	_____
. 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?	_____	_____

	Yes	No
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

	Yes	No
22. Have you completed the statistical return on complaints and dispute resolution in Part C?	_____	_____
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?	_____	_____
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 the Schedule to the Code?	_____	_____
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	_____	_____

	Yes	No
- 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) If the investigation continued beyond 45 days, did you provide the cardholder with:		
. monthly updates of its progress: and	_____	_____
. a date when a decision can reasonably be expected?	_____	_____
27(b) 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?	_____	_____
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?	_____	_____

	Yes	No
29a) 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?	_____	_____
31. Did you resolve complaints in the customer's favour if your staff did not comply with the Code?	_____	_____

Yes **No**

SECTION 3: PRIVACY

32. Did your procedures require staff to comply with the principles in relation to privacy as set out below:		
(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?	_____	_____

	Yes	No
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
GUIDELINES FOR E.F.T. SECURITY
IMPLEMENTATION ASSESSMENT

Guideline	Yes/No	Comments ³⁸
1. Positioning of EFT devices where customer PIN entry is required: (a) Have you adopted this Guideline as policy?
(b) Have you incorporated this Guideline into your procedures, controls and internal audit/assessment processes?
(c) Are there any aspects of this Guideline where further action is proposed?
2. EFT customer education: (a) Have you adopted this Guideline as policy?
(b) Have you incorporated this Guideline into your procedures, controls and internal audit/assessment processes?
(c) Are there any aspects of this Guideline where further action is proposed?

³⁸ Comments from institutions will assist ASIC in identifying any areas of difficulty in the implementation of the Guidelines and in assessing their on-going suitability.

Guideline	Yes/No	Comments ³⁹
3. Management of cryptographic keys for the protection of transactions:	
(a) Have you adopted this Guideline as policy?
(b) Have you incorporated this Guideline into your procedures, controls and internal audit/assessment processes?
(c) Are there any aspects of this Guideline where further action is proposed?

³⁹ Comments from institutions will assist ASIC in identifying any areas of difficulty in the implementation of the Guidelines and in assessing their on-going suitability.

PART C

COMPLAINT RESOLUTION ASSESSMENT

INSTITUTION:PERIOD:
1/4/1999 - 31/3/2000

A.	EFT Transactions									
	TOTAL NUMBER IN PERIOD									
B.	Transactions Complaints Resolution Data									
	TYPE	<u>Total</u>	+	<u>Complaints held over</u>	=	<u>Issuer liable</u>	+	<u>Customer liable</u>	+	<u>Complaints outstanding</u>
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 <u>not</u> lost or stolen	_____	
	(c) Other	_____	
	TOTAL	_____		_____		_____		_____		_____
3.	OTHER									
	(a) Confusion over merchant name and/or processing date	_____		_____		_____		_____		_____
	(b) Double debit transactions	_____		_____		_____		_____		_____
	TOTAL LIABILITY COMPLAINTS	_____	+	_____	=	_____	+	_____	+	_____

C.	Unauthorised transactions where customer liable for at least part of loss	<u>Number</u>
	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) ATM deposit shortfall
	(b) Investigation terminated (at customer's request or due to loss of contact)
	(c) Evidence of fraud or other offence
	TOTAL (Equals the total of "Customer liable" column in B2 above)	_____
D.	Unauthorised transactions where issuer liable	<u>Number</u>
	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)	_____

E.	Privacy	<u>Total</u>	+	<u>Complaints held over</u>	=	<u>Complaints resolved to customer's satisfaction</u>	+	<u>Complaints not resolved to customer's satisfaction</u>	+	<u>Complaints outstanding</u>
	Complaints about privacy in EFT transactions	_____		_____		_____		_____		_____