


ASIC

Australian Securities & Investments Commission

REPORT 63

# Compliance with the EFT Code of Conduct

# (April 2003 to March 2004)

December 2005

# Executive Summary

This report gives the results of the annual monitoring of the Electronic Funds Transfer Code of Conduct (EFT Code). The monitoring period was 1 April 2003 to 31 March 2004.

This report contains information on:

- Code membership;
- Code compliance;
- Code administration; and
- Code-related complaints.

Since the revised EFT Code came into operation in 2002 there have been problems associated with data collection and quality. Because of this, only limited comparisons are made with previous reporting periods and these are highly qualified. ASIC is working with subscribing institutions to improve the quality and comparability of monitoring data.

Despite the data collection problems, as in previous years, reported levels of compliance with the EFT code remain high overall. The reported numbers of complaints per million transactions was 55 although the lack of data provided in some instances means that this figure may be under or over stated and making trend comparisons on this issue would be unwise.

Most EFT subscribers completed (or partly completed) the monitoring survey for the period. Some reported non-compliance was the result of computer systems issues, not all of which were able to be resolved during the monitoring period. There were also issues related to the interpretation of survey questions that resulted in some responses being unreliable. Those reported breaches of the EFT Code that cause ASIC particular concern are highlighted in the report, and we will be following up with the institutions concerned.

EFT subscribers also continued to have trouble providing complaints statistics in the form we now ask for them – that is broken down by delivery channel. Those who were able to report complaints statistics recorded 138,775 EFT complaints and 2.5 billion EFT transactions for the period.

Overall, most complaints (71%) were resolved in favour of the customer. ATM cash dispensing problems were the most common source of complaints.

## Reading this report

ASIC monitors compliance against the specific clauses of the EFT Code. Ideally, this report should be read in conjunction with the EFT Code itself, and throughout the report we have identified the relevant clauses as a guide for readers.

# Contents

**EXECUTIVE SUMMARY** ..... **2**

READING THIS REPORT ..... 3

**CONTENTS** ..... **4**

**ABOUT THE EFT CODE** ..... **5**

**ABOUT THE EFT CODE MONITORING** ..... **7**

OVERVIEW OF PROCEDURE ..... 7
WHAT IS A "COMPLAINT" UNDER THE EFT CODE? ..... 7
FUTURE EFT CODE MONITORING ..... 7

**MONITORING RESULTS** ..... **9**

CODE MEMBERSHIP AND RESPONSES ..... 9
OVERALL COMPLIANCE WITH THE EFT CODE ..... 9
EFT COMPLAINTS ..... 17

**APPENDIX A: EFT CODE SUBSCRIBERS** ..... **29**

**APPENDIX B: METHODOLOGY** ..... **30**

MONITORING INSTRUMENT AND PROCEDURE ..... 30
CHANGES TO SURVEY DESIGN ..... 30
DATA QUALITY ..... 31

**APPENDIX C: EFT CODE MONITORING SURVEY QUESTIONS (PART A – CHECKLIST)** ..... **33**

**FURTHER INFORMATION** ..... **43**

# About the EFT Code

The Electronic Funds Transfer Code of Conduct ('EFT Code') is a voluntary code of practice covering consumer electronic funds transfer services. Subscribing institutions agree to comply with the requirements of the Code in their Terms and Conditions for EFT transactions.

The EFT Code plays a central role in promoting consumer confidence in electronic transacting. Banks, building societies and credit unions offering consumer electronic funds transfer services in Australia have all traditionally subscribed to the Code. ASIC strongly encourages all institutions that provide products and services covered by the Code, including new entrants that are not traditional deposit taking institutions, to formally subscribe to it.

The EFT Code has operated since 1989. The current revised EFT Code was issued in April 2001 and commenced operation in March 2002. The EFT Code will undergo further review in 2005/06.

The EFT Code has three parts:

- Part A covers the 'rules and procedures to govern the relationship between users and account institutions in electronic funds transfers involving electronic access to accounts'[1];
- Part B covers the 'rules for consumer stored value facilities and stored value transactions'[2]; and
- Part C covers 'privacy, electronic communication, administration and review'.[3]

The types of transactions covered by the EFT Code include:

- ATM transactions;
- EFTPOS transactions;
- Telephone and internet banking transactions;
- Credit card transactions that do not require a signature for authentication (for example those used over the phone and/or internet);
- Wireless Application Protocol (WAP) transactions; and
- Stored value product transactions.

[1] EFT Code p4.

[2] EFT Code p22.

[3] EFT Code p29.

Key areas covered by the EFT Code include:

- Disclosure of Terms and Conditions, and changes to Terms and Conditions;
- Transaction records and periodic statements;
- How liability for disputed transactions is allocated and the nature or extent of that liability;
- Requirements for handling complaints;
- Privacy and security obligations;
- The need for an audit trail; and
- Rights in relation to stored value facilities and transaction.

Further information about the EFT Code, including a copy of the Code itself and a consumers' guide to the code, is available from ASIC's consumer web site FIDO:

http://www.fido.gov.au/codes

# About the EFT Code monitoring

Institutions that subscribe to the EFT Code ('subscribers') are surveyed annually to monitor their compliance with the Code. ASIC has undertaken this monitoring since 1998.

## Overview of procedure

The survey is sent to subscribers in early April and relates to the previous year (1 April to 31 March). The monitoring period referred to in this current report is 1 April 2003 to 31 March 2004 ('the reporting period').

The survey questions are divided into two main sections:

- Part A: Code of conduct checklist; and
- Part B: Complaints statistics.

The Credit Union Services Corporation (Australia) Limited (CUSCAL) submits aggregated monitoring data to ASIC on behalf of all its affiliated credit unions (referred to as '*CUSCAL credit unions'* in this report). Credit unions that are not CUSCAL affiliates ('*credit unions'*) and all remaining institutions (i.e. '*banks'*, '*building societies'* and '*other institutions'*) submit individual monitoring surveys to ASIC directly. The category '*other institutions'* includes third party providers (i.e. not account institutions) and finance companies.

The findings of the survey are released in a report that is made publicly available via ASIC's website. The last report (1 April 2002 to 31 March 2003) was withheld due to poor quality data. This was largely a consequence of the expanded scope of the Code post April 2002.

In response to some of these problems, ASIC simplified the survey used for this reporting period, in particular the complaints information.

Please refer to Appendix B for the full methodology.

## What is a "complaint" under the EFT Code?

EFT Code subscribers must report on all complaints about matters falling within the EFT Code where the issue of liability arises, or may arise. This includes *all* EFT-related complaints, not just those that become "disputes". That is, institutions must report on EFT complaints that were settled immediately, as well as those that took longer to resolve.

## Future EFT Code monitoring

ASIC is currently reviewing the EFT Code monitoring process to identify ways to improve the quality and comparability of the data, in

particular the data about EFT transactions and complaints. ASIC is concerned that many subscribers are currently not meeting their reporting obligation under clause 10.14[4] of the Code and we are working with them to remedy this. Part of the solution may require subscribers to change their data collection systems. We accept that not all institutions will be able to implement these changes immediately.

As a result there may be at least one more year in which ASIC will not release a full public report on compliance with the EFT Code. Institutions will still be required to report non-compliance with the EFT Code to ASIC during this period.

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

# Monitoring results

## Code membership and responses

The EFT Code is open to any type of institution offering transaction mechanisms covered by the Code. Currently all Code subscribers (apart from two third party service providers[5]) are financial services providers – banks, building societies, credit unions and finance companies.

There were 185 subscribing institutions that responded to the survey. One *bank* and a small number of *CUSCAL credit unions* did not submit a completed and verified survey. ASIC will be following up this non-compliance with these institutions.[6] A list of subscribers is provided in Appendix A.

## Overall compliance with the EFT Code

### About Part A checklist

The Part A checklist surveyed Code subscribers about their compliance with the EFT Code of Conduct. Survey questions were based directly on the provisions of the EFT Code. Institutions were able to provide comments to explain their answers.

### Number and quality of responses

Forty-six individual Code subscribers submitted the Part A checklist to ASIC for the April 2003 to March 2004 period. Three found that most of the questions did not apply to their institution.[7] An aggregate response was received on behalf of 139 *CUSCAL credit unions*, which included breakdowns on, for example, the numbers of credit unions complying or not complying with each provision.

There were some issues with the clarity of survey questions and the compliance statistics should therefore be interpreted cautiously. Where possible, the researchers have used the comments made by institutions to interpret the responses and adjustments have been made accordingly. These cases have been footnoted.

---

[5] Cashcard and First Data.

[6] After the deadline, American Express International submitted a partly completed softcopy version of the survey, noting a lack of confidence in the validity of the statistics. A further extension failed to produce a final version of the survey response. A small number of *CUSCAL credit unions* did not submit data as part of CUSCAL's aggregated survey.

[7] Refer to Appendix B for further information about data quality.

## Terms and Conditions

*Availability and disclosure of Terms and Conditions [Part A, clause 2]*

Institutions indicated a high level of compliance with this clause.

One *CUSCAL credit union* did not include a warranty that the requirements of the EFT Code would be complied with in its brochures for phone and internet banking [clause 2.1]. ASIC considers that any failure to include this warranty in product Terms and Conditions represents a serious breach of the EFT Code.

One *other bank* said that it had not provided prior information to customers about charges for the issue or use of an access method [clause 2.3(a)] because its customers were charged fees based on the volume of transactions they made:

> *"For example, a customer may receive a certain number of ATM transactions each month without being charged and once this limit is reached they will be charged a fee for all subsequent transactions*."[8]

We believe that institutions should still be able to itemise these fees in accordance with the EFT Code. For example, they can say how many fee-free transactions are allowed before the fee applies).

*Changing the Terms and Conditions of use [Part A, clause 3]*

Fifty-five institutions (30%) said they changed their Terms and Conditions in the reporting period. Half of the institutions that changed their Terms and Conditions were *CUSCAL credit unions*.

Two *CUSCAL credit unions* said that they failed to give customers at least 20 days written notice of changes to Terms and Conditions that increased a customer's liability for losses relating to EFT transactions [clause 3.1(b)]. No explanation for this failure was provided. ASIC will follow up with them.

## Records of EFT transactions and notice of surcharges

*Receipts [Part A, clause 4A]*

A number of breaches were reported. We have separated the following findings about "voice communications" (e.g. telephone banking) and "non-voice communications" (e.g.written receipts).

[8] The *other bank* answered N/A to the question, but the response in their comments described why they did not comply and was treated as No.

### Voice communications

Nine institutions (5%) said that they did not provide customers with a receipt number at the time of the transaction [clause 4.1(b)(i)]. The only explanatory comment was by one *building society* that said it did not give receipt numbers where the transfer was within the institution. In ASIC's view it is important that consumers always get a receipt number so that they are able to keep track of their transactions, and verify these against their statements.

Twenty-one institutions (11%) did not provide customers with the name of the merchant who received payment for EFT transactions [clause 4.1(b)(v)]. A biller code rather than the merchant's name was provided in most cases.

ASIC would prefer the merchant name to be provided. However we have previously advised that identification by biller code will suffice for compliance, as long as the merchant's customer invoice clearly sets out both the merchant's name and the relevant biller code. This is an issue that we will raise in the next review of the EFT Code.

Twenty-six institutions (14%) said that they did not provide customers with the balance remaining in the account at the time of the transaction [clause 4.1(b)(vi)]. The main explanation was that the balance could be obtained by other phone banking options (e.g. by returning to the main menu after the transaction and selecting ‘account balance’). ASIC is satisfied with this, provided that getting the balance information does not give rise to separate charges.

### Non-voice communications

Twenty-five institutions (14%) said that they did not issue receipts showing the balance remaining in the account at the time of the transaction. One explanation provided by several institutions was that:

- Some internet software systems did not provide balances when the transaction was made, but balances were available via a separate screen once the transaction was completed *(CUSCAL credit unions, bank and other bank).*

Another explanation provided by several institutions was that:

- The transaction receipt was printed in duplicate for EFT transactions and printing the balance on the receipt would compromise customer privacy (with the merchant being made aware of the customers account balance) *(bank and credit union).*

Clause 4.1(a)(viii) provides an exemption for the above instance. Balance information does not need to be provided if it would

compromise a customer's privacy and there is no breach in these circumstances.

### *Periodic statements [Part A, clause 4B]*

Twenty-five institutions (14%) said they did not identify charges relating to the use of an access method as a separate item on statements [clause 4.3(b)]. Explanations included:

- Fees were accumulated and charged at the end of each month and were not split into transaction types *(building societies and a credit union)*;
- Individual information was available to customers on request *(building society)*; and
- A dollar allowance was provided to customers, and all fees for the month were totalled and any excess was charged to the customer, so this was the only figure shown on the statement *(building society).*

The explanation provided on behalf of the seventeen *CUSCAL credit unions* in this category was that the charges were:

> *'… separately calculated but are offset by a loyalty rebate and a net charge "Excess Withdrawals" appears on statements'.*

ASIC is concerned about these breaches. Itemised fee information on statements is important so that consumers can check the accuracy of the charges and better manage the costs of their transacting. We will follow up with these institutions.

### *Security advice [Part A, clause 4C]*

Thirteen institutions (7%) said they did not include in or with account statements a 'clear, prominent and self-contained statement summarising security guidelines for access methods' at least annually [clause 4.5]. These institutions did not provide satisfactory explanations for this non-compliance and ASIC will follow up with them.

### *Notice of surcharges for using "foreign" electronic equipment [Part A, clause 4D]*

Clause 4.6 states that account institutions must have, in their agreements with merchants, a requirement that the merchant disclose any direct charge that they impose on a consumer for making an electronic transaction. This information must be disclosed *before* the consumer goes ahead with the transaction. An example would be a dollar surcharge

imposed by a retailer for credit card transactions. In that case a handwritten, prominent sign at the cash register would suffice.

Seven institutions (4%) said they did not include this requirement in their agreements. We will follow up with these institutions. One *other bank* explained that new and existing EFTPOS merchant agreements are being amended to include this requirement.

## Complaints investigation and resolution procedures

**[Part A, clause 10]**

Clause 10.6(c) says that if a subscriber cannot resolve a complaint within 45 days of receiving it, then it must specify a date when a decision can reasonably be expected. Four institutions (2%) said that they did not specify such a date. The only explanation provided for non-compliance was by one *credit union* that said they kept the member informed. The three *CUSCAL credit unions* in this category provided no explanation. Again, we will follow this up with the institutions involved.

### *Complaints concerning credit or charge cards*

Where credit card or charge card account complaint resolution was sought under the rules of the respective card scheme, six institutions (12% of the 52 institutions that reported receiving complaints about credit cards) said that they did not suspend the account holder's obligation to pay the complaint amount and any credit - and other charges related to that amount - until the complaint was resolved. Under clause 10.7(c)(ii) the institution is also required to inform the customer of the payment suspension. Explanations provided were:

- The disputed transaction was automatically suspended, but, interest was only suspended for the current statement cycle *(major bank)*;
- The amount was refunded on resolution *(other bank)*;
- Refunds were backdated, fees and interest were adjusted and telephone updates were given to customers *(other bank)*;
- Suspension of the account holder's obligation to pay was not deemed necessary *(credit union)*; and
- Any additional payments, interest, fee or charges incurred due to the complaint were reimbursed after the investigation if the outcome was in favour of the customer *(building society)*.

This may also be a breach of card scheme chargeback rules. We will follow up with the relevant institutions.

*EDR scheme members*

Four members of external dispute resolution ('EDR') schemes (2% of all respondents) said that they did not inform their customers of the right to lodge a complaint with the EDR scheme within five business days of the relevant time period expiring [clause 10.8]. Explanations included:

- *'If there are any delays in resolution, we continue to communicate with our clients in order to work towards resolution without reference to EDR. This includes regular contact, progress updates and expected completion dates' (other bank).*

Six *CUSCAL credit unions* (4% of all *CUSCAL credit unions*) said that they did not promptly inform the customer of the complaint investigation outcome reasons including references to the relevant clauses of the EFT Code, when an investigation was completed [clause 10.9(b)]. No explanation for this failure was provided.

ASIC believes knowledge about dispute resolution issues is extremely important and will be following up these breaches with the institutions involved.

Two institutions (1% of all respondents) failed to make available copies of documents or other evidence (including information from relevant ATM logs or audit trails), following an investigation in which account holders were held liable for at least part of the disputed of transaction amount [clause 10.11(a)]. The *CUSCAL credit union* was in the process of making changes to its member letter to advise about the availability of evidence. The *credit union* explained:

> *'We make claims on behalf of our members for transactions made on other institutions ATM or EFTPOS devices. For the claims that were denied by the other institution no evidence was provided other than the correspondence advising the decline. In this case we simply advised our member that the claim was denied, the reason the claim was denied and provided them with the required information if they wanted to take the complaint/ claim further. We do not own or operate any ATM or EFTPOS devices and therefore cannot provide this evidence first hand.'*

## Stored value facilities [Part B, clauses 11 – 19]

Only one institution (1% of all respondents) reported offering a stored value facility or transactions (one *other bank* and one *credit union*). This shows that sign-up to the Code for providers of stored value facilities remains low and that few existing members are offering such products.

*Refund of lost or stolen stored value*

The *other bank* failed to pay the user the amount of stored value that it could have prevented from being transferred from the facility where a user gave the bank notice of the loss or theft of the stored value facility, because:

> *'Our Terms and Conditions state that if the card is lost the funds are like cash. Anyone who has possession of the card can use the card. We cannot restrict use of lost cards.'*

If the *other bank* had the capacity to prevent further loss then they were in breach of clause 16.1 of the Code. We will take this issue up with them**.**

### Privacy [Part C, clause 21]

Eighteen institutions (10%) did not audit or review compliance with the National Privacy Principles in the *Privacy Act* 1988 Commonwealth or with a code that had been approved and was operative under that legislation. Fifteen of those institutions were *CUSCAL credit unions* that did not provide any explanation for this

The most recent audit by one of the *other banks* was in February 2003 and a *credit union* had last been audited in March 2002.

### Staff training on the requirements of the Code [Part C, clause 23]

*On-the-job training*

Most institutions (98% of all respondents) used procedures manuals for EFT training.

Most institutions (96%) also used passive on-the-job EFT training.[9] Exceptions were one *other bank* and four *CUSCAL credit unions*. The *other bank* provided a self-paced training workbook and competency test to staff and used internal memos and an intranet site to communicate procedural changes. Their support unit provided staff with the Electronic Banking Terms and Conditions.

The use of video for on the job EFT training was less common, with 69 institutions (38%) using this method. Video use was more prevalent among *CUSCAL credit unions*, with nearly 50% using this training method. Apart from *CUSCAL credit unions* only two *other banks* and one *credit union* used video training. Some institutions noted they used

[9] The sample size in this question (and the remainder of questions in this section) is 180, as responses to this question were received by 134 rather than 139 *CUSCAL credit unions*

other methods instead as they did not believe video training was necessary for compliance with the EFT Code.

The use of active on the job training such as team meetings was common with 96% using this method. The only exceptions were one *credit union* and four *CUSCAL credit unions*.

126 institutions (70%) used testing as a method of on the job EFT staff training. The exceptions were thirty-eight *CUSCAL credit unions* (28% of *CUSCAL credit unions*), five *building societies*, three *credit unions*, two *major banks*, two *minor banks* and one *other institution*. Explanations included that testing was not considered necessary and that staff performance reviews were regularly undertaken.

### *External training*

85 *CUSCAL credit unions* (63% of 134 *CUSCAL credit unions*) used external training for their EFT staff training compared with seventeen (37%) of the forty-six remaining institutions.[10] One *other bank* noted the use of the Banking and Financial Services Ombudsman as an external provider of EFT Code staff training. Many institutions explained they used in-house training rather than external training.

### *Other EFT staff training methods*

More than half the institutions said they used other methods for EFT staff training, which included:

- Compliance manuals;
- Staff presentations;
- Training modules (via staff inductions, group training sessions, online training and refresher training);
- Communication regarding procedural changes provided via internal memos, intranet sites and staff bulletins (including e-circulars); and
- Sending customer relations staff to the annual conference of the Banking and Financial Services Ombudsman.

[10] The sample size in this question is 180, as responses to this question were received by 134 rather than 139 *CUSCAL credit unions*

## EFT Complaints

EFT Code subscribers must provide information about complaints as part of the monitoring exercise. They must report on the number, type and resolution of relevant complaints. They are also asked to report the number of EFT transactions recorded for the period. This section of the report presents the aggregated complaints and transaction information.

### Breaking down complaints and transaction data

Prior to its most recent revision, the EFT Code covered only ATM and EFTPOS transactions. Now that the Code covers the full range of electronic transactions (e.g. including internet and phone banking), ASIC believes it is important that subscribers collect and report complaints and transaction data according to delivery channel. Most Code subscribers tell us that they do not yet have the systems in place to do this. ASIC is continuing to consult with industry about this.

### Number and quality of responses

ASIC analysed 181 complaints responses (refer to Table 1).

**Table 1: Complaints analysis sample information**

| | Major Bank | Other Bank | Building Society | Credit Union | Other Institution | Total |
|---|---|---|---|---|---|---|
| **Returned survey** | 4 | 11 | 11 | 154 | 5 | 185 |
| Returned full or partial complaints data | 4 | 11 | 11 | 154 | 3 | 183 |
| Excluded from complaints analysis* | 0 | 1 | 0 | 0 | 1 | 2 |
| **Complaints analysis sample** | 4 | 10 | 11 | 154 | 2 | 181 |

Notes to table:

*Excluded due to very limited and/or incompatible data.

As Table 1 shows, we received full or partial complaints data from 183 of the 185 institutions that returned a survey. The two *other institutions* that did not supply complaints data are both third party service providers (i.e. not account institutions) that do not manage EFT complaints directly. Of the 183 remaining surveys, we excluded the very limited and/or incompatible data provided by two institutions (an *other bank* and an *other institution*), leaving a final complaints analysis sample of 181 institutions.

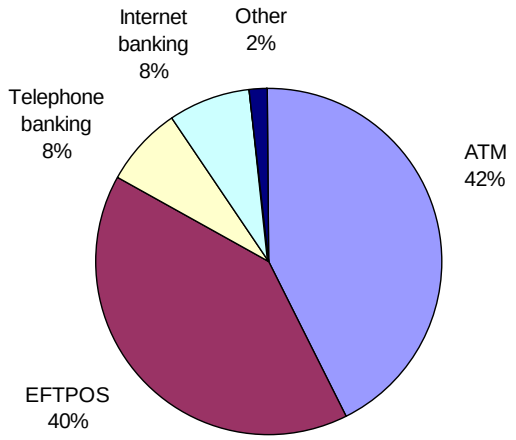
The two *other institutions* included in the complaints analysis sample are both finance companies.

Given that CUSCAL only provided partial complaints information on behalf of its 139 affiliates, and several of the remaining institutions also omitted information required in the complaints part of the survey, there were relatively few full responses among the final sample of 181. This year's results should therefore be interpreted cautiously and, in general, treated as an underestimation of *actual* EFT transactions and complaints. Where possible, the researchers have qualified incomplete samples in the corresponding table notes. Please also refer to Appendix B for further information about data quality.

## Total EFT transactions

Institutions reported 2.5 billion EFT transactions in the year to 31 March 2004.[11] As Chart 1 shows, ATM and EFTPOS transactions exceeded other types of EFT transactions. However, several institutions (particularly larger institutions) had difficulty reporting telephone and internet transactions. Therefore, telephone and internet transactions are probably understated in Chart 1.

**Chart 1: Total number of EFT transactions**




Notes to chart:

Some institutions, including some of the *major banks*, were unable to split transaction figures by delivery type. Internet banking and phone banking proved particularly difficult and so may be understated in this chart. Some institutions used the 'other' category when phone and internet transactions could not be separately reported but others omitted phone and/or internet statistics altogether.

[11] Exact figure: 2,529,550,988.

To put the above figures in context, Table 2 shows the results of ANZ's 2003 financial literacy research, in which participants were asked to indicate which payment methods they used.

**Table 2: ANZ consumer research on payment methods used**

**A1. There are various ways of paying for goods and services. Which of the following payment methods do you, yourself, use?**

**A2. IF DOESN'T USE, ASK: What other payment methods do you know how to use, even if you don't use them yourself?**

| Payment method | % of all adults using | % of all adults using or knowing how to use | % of those who know about method that use it |
|---|---|---|---|
| Cash | 96 | 100 | 96 |
| ATMs | 73 | 91 | 80 |
| Cheques | 46 | 91 | 51 |
| EFTPOS | 71 | 89 | 80 |
| Credit Cards | 64 | 89 | 72 |
| Laybys | 27 | 83 | 33 |
| Money orders | 20 | 82 | 24 |
| Direct debit | 50 | 78 | 64 |
| Loans | 35 | 71 | 49 |
| Store cards | 15 | 71 | 21 |
| Telephone banking | 36 | 68 | 53 |
| Debit cards* | 34 | 68 | 50 |
| Bpay | 36 | 60 | 60 |
| Internet banking | 28 | 52 | 54 |

Notes to Table:

Base: Total Respondents

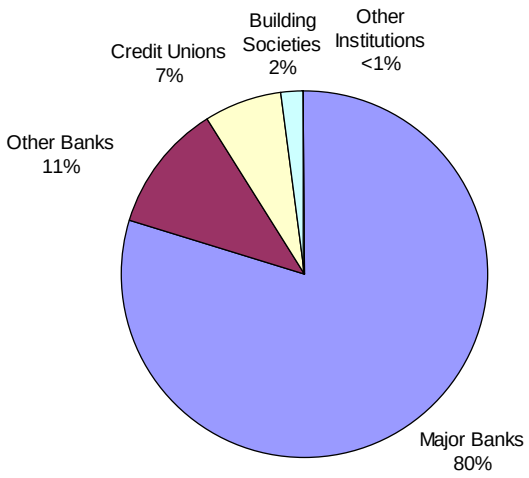
Sample Size: 3,548

*The proportion of people using debit cards is almost certainly understated due to respondents' perceptions. The majority of respondents using ATMs and EFTPOS would have been using a debit card, but appear not to recognise it as such.

*Source: ANZ SURVEY OF ADULT FINANCIAL LITERACY IN AUSTRALIA - STAGE 2: TELEPHONE SURVEY REPORT (April, 2003)*

As indicated in Chart 2, the *major banks* reported most (80%) of the EFT transactions recorded this period.

**Chart 2: Total EFT transactions by institution type**




Notes to chart:

As indicated in Chart 1, some institutions, including some of the *major banks*, experienced difficulty providing accurate transactions statistics.

## Total EFT Complaints

A total of 138,775 EFT complaints were recorded during the reporting period. However, this is an underestimation of complaints because, as outlined above, two institutions were excluded from the analysis, the largest *other bank* did not report their total complaints figures and several other institutions, including some of the *major banks*, under-reported their complaints figures due to systems barriers.

**Table 3: Total number of EFT transactions and complaints by year**

| Year | Number of complaints (including those held over from previous year) | Number of Transactions | Complaints per million transactions |
|---|---|---|---|
| 2003/2004 | 138,775* | 2,529,550,988** | 55 |
| 2002/2003*** | | | |
| 2001/2002 | 132,517 | 1,640,586,411 | 81 |
| 2000/2001 | 121,434 | 1,499,786,422 | 81 |
| 1999/2000 | 106,719 | 1,655,373,445 | 64 |
| 1998/1999 | 73,125 | 1,710,904,716 | 42 |

Notes to table:

There have been modifications to the survey design since 2002. These, along with more minor alterations to the survey, may have affected the comparability of these results.

*This total understates the true number of complaints due to nil reporting of this particular figure by a small number of institutions, including the largest *other bank,* and under-reporting by several other institutions, including some of the *major banks* (who most commonly under-reported internet and phone banking complaints).

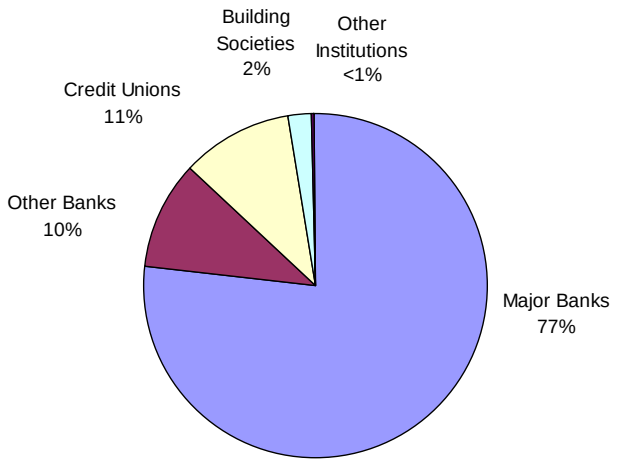
**The rise in transactions in part reflects the broadened focus of the revised EFT Code. As noted in Chart 1, some institutions, including some of the *major banks*, were unable to split transaction figures by delivery type and omitted these figures in their survey.

***Due to the poor quality of data received, figures were not reported for this period.

While it is difficult to verify due to poor quality data, it would appear that there continues to be less than 100 complaints per million transactions.

As shown in Chart 3, the *major banks* reported the majority of EFT complaints recorded during the reporting period, which is unsurprising given they also recorded the most EFT transactions (see Chart 2).

**Chart 3: Total EFT complaints by institution type**




Notes to chart:

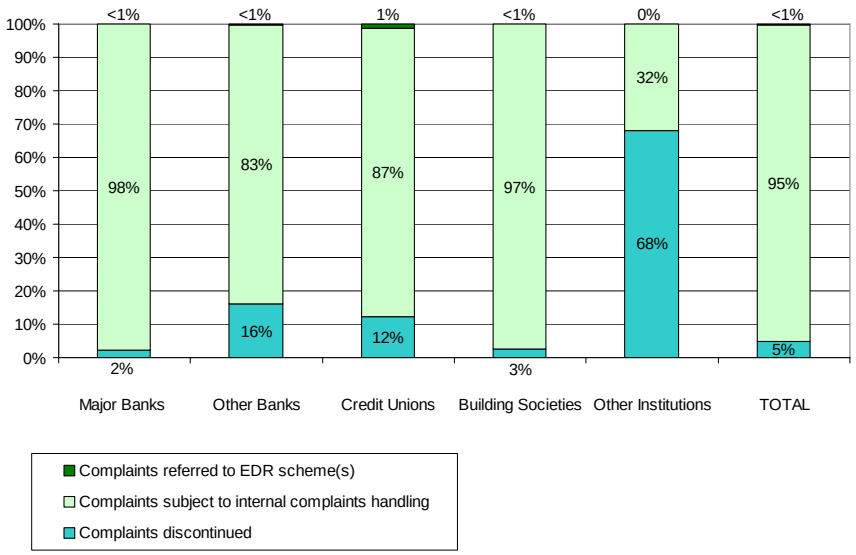
The proportion of complaints recorded by *other banks* is distorted due nil reporting of this particular figure by two *other banks*, including the largest *other bank.*

The proportion of complaints recorded by *credit unions* and *major banks*, is distorted due to under-reporting (especially in terms of phone and internet banking complaints).

## EFT complaint handling

As shown in Chart 4, most institutions recorded very small proportions of complaints referred to EDR and small to medium proportions of complaints that were, for whatever reason, discontinued. *Other institutions*, however, reported a disproportionately high number of these discontinued complaints. This appeared to be due to one institution in particular. ASIC will follow up this anomaly with the institution directly.

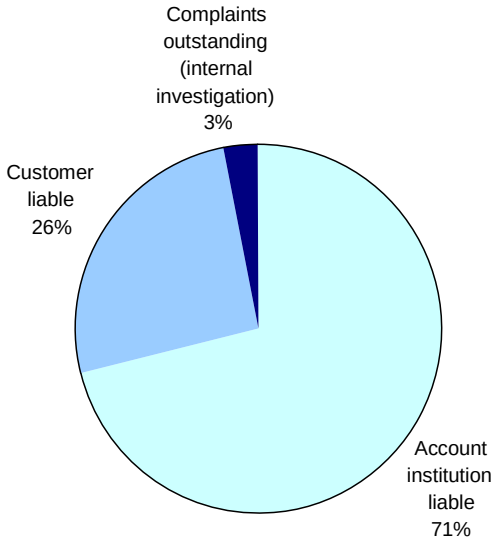
**Chart 4: Complaint handling status by institution type**



## EFT complaint resolution

Chart 5 shows that, at an aggregate level, most of the complaints that were subject to internal complaints handling were resolved in favour of the customer (i.e. the institution was found liable in most (71%) of cases). These findings are consistent with previous years.

**Chart 5: Resolution of EFT complaints subject to internal complaints handling**




Notes to chart:

At least one institution included under 'Account institution liable' complaints in which another institution was ultimately found liable, not their own institution. Some institutions may have omitted these kinds of complaints.

While institutions were more likely to be found liable than customers at the aggregate level, liability trends did vary according to the nature of the complaint, as shown in Table 4.

Unsurprisingly, customers were less likely to be found liable in a case of system malfunction than in a case of an unauthorised transaction. This is in line with results in earlier years.

**Table 4: Type of EFT complaint by resolution**

| Complaint type | Number of internally handled complaints* | Resolution | | |
|---|---|---|---|---|
| | | Account institution liable | Customer liable | Not yet resolved (outcome pending) |
| System malfunction | | | | |
| ATM cash dispensing problem | 85,382 | 84% | 12% | 3% |
| Other system malfunction (i.e. system failed to complete transaction with customer's instructions) | 12,133 | 78% | 12% | 11% |
| Unauthorised transactions | | | | |
| Device and/or access method lost or stolen, or security breached | 18,802 | 57% | 42% | 2% |
| Device and/or access method NOT lost or stolen, or security breached | 34,829 | 72% | 28% | <1% |
| Double debit transactions** | 3,339 | 70% | 27% | 4% |
| Confusion over merchant name or processing date | 6,904 | 7% | 93% | <1% |

Notes to table:

*This complaints breakdown is not designed to correspond with the earlier quoted total EFT complaints figure of 138,775.

**A double debit transaction is one where the same transaction seems to have been processed twice.

The liability trends varied somewhat by institution type. A summary of these variations is provided below.

*ATM cash dispensing problem*

*Other institutions* were the only institution type to resolve in favour of the institution more often than the customer. Their proportion of customer liable was much higher than remaining institutions:

- *Other institutions* found customers liable in 52% of cases.
- Remaining institutions found customers liable in 6% – 13% of cases (*building societies* were least likely to find customers liable).

To keep the above trends in perspective, there were only two *other institutions* in this sample, and they accounted for a negligible 0.2% of all EFT complaints reported during the period. Just one of the two appeared to favour institutions more frequently than customers. ASIC will be talking to them to better understand why their results were so anomalous.

*Other system malfunction (i.e. system failed to complete transaction with customer's instructions)*

*Other institutions'* proportion of customer liable was higher than remaining institutions though, as explained above, this divergence should be viewed in context:

- *Other institutions* found customers liable in 35% of cases.
- Remaining institutions found customers liable in 5% – 26% of cases (*building societies* were least likely to find customers liable).

*Device and/or access method lost or stolen, or security breached*

*Other institutions* were the only institution type to resolve in favour of the institution more often than the customer. Their proportion of customer liable was higher than remaining institutions, but only marginally higher than *major banks*:

- *Other institutions* found customers liable in 50% of cases (they found the institution liable in 42% of cases and 8% of cases were outstanding).
- *Major banks* found customers liable in 49% of cases (they found the institution liable in 50% of cases and 1% of cases were outstanding).
- Remaining institutions found customers liable in 19% – 32% of cases (*other banks* were least likely to find customers liable).

*Device and/or access method NOT lost or stolen, or security breached*

*Major banks* were the only institution type to resolve in favour of the institution more often than the customer. Their proportion of customer liable was much higher than remaining institutions. ASIC will follow up this trend with the major banks.

- Major banks found customers liable in 78% of cases.
- *Other institutions* did not report any complaints in this category.
- Remaining institutions found customers liable in 2% – 23% of cases (*building societies* and *other banks* equally were the least likely to find customers liable).

*Double debit transactions:*

All institutions resolved in favour of the customer more often than the institution, except *other institutions*, which favoured both equally. The proportion of customers liable was higher among *major banks* and *other institutions* than for remaining institution types:

- *Major banks* found customers liable in 41% of cases.
- *Other institutions* found customers liable in 40% of cases.
- Remaining institutions found customers liable in 0% – 12% of cases (*building societies* were the least likely to find customers liable).

*Confusion over merchant name or processing date*

All institutions resolved in favour of the institution more often than the customer, except *other institutions*, which reported no complaints in this area. The proportion of customer liable was higher among *major banks* than for remaining institution types:

- *Major banks* found customers liable in almost all (99.7%) of cases.
- Remaining institutions found customers liable in 61% – 85% of cases (*other banks* were the least likely to find customers liable).

This result is consistent with previous findings, and we understand that consumer confusion is usually at the heart of these complaints. For example, where the processing date of the transaction (shown on a statement) is different from the *actual* date of the transaction.

## Customer liability limited to $150

This limitation applies when a PIN or password was required to perform an unauthorised transaction, but where the institution cannot prove that the customer contributed to the loss. As indicated in Table 5, liability is currently limited to $150. Prior to the last EFT Code revision in 2001 the figure was $50.[12]

**Table 5: Customer liability limited**
**(Limited to $150 since 2002/2003 and limited to $50 prior to 2002/2003)**

| | Total complaints | Customer liability limited to $150 | Customer liability limited to $50 | Percentage of Total complaints |
|---|---|---|---|---|
| 2003/2004 | 138,775 | 1,428 | n/a | 1% |
| 2002/2003* | | | | |
| 2001/2002 | 132,517 | n/a | 456 | <1% |
| 2000/2001 | 121,434 | n/a | 1,167 | 1% |
| 1999/2000 | 106,719 | n/a | 2,506 | 2% |
| 1998/1999 | 73,125 | n/a | 675 | 1% |

Notes to table:

In 2002 the liability limit increased from $50 to $150. With the 2002 revisions to the EFT Code not only was monetary cap changed but also the burden of proof.

There have been modifications to the survey design since 2002. These, along with more minor alterations to the survey, may have affected the comparability of these results.

Due to statistical errors and under-reporting by most credit unions, the true number of limited liability cases may be understated in this table.

*Due to the poor quality of data received, figures were not reported for this period.

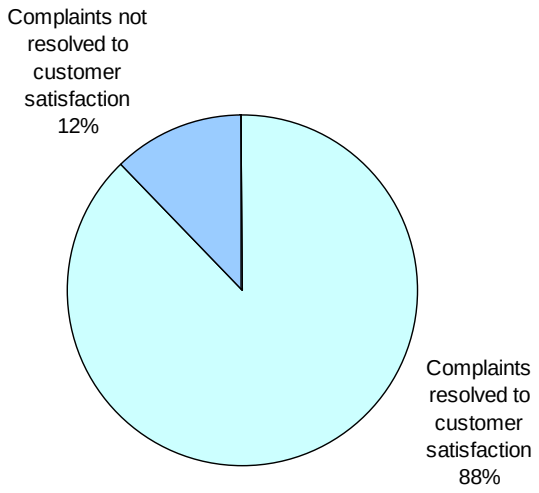
The big four banks reported the highest proportion of complaints that resulted in customer liability being limited to $150 (91%). However, due to statistical errors and considerable under-reporting by most credit unions, it is unclear whether the big four banks are actually the most likely of all EFT Code subscribers to settle complaints in this way.

[12] The current version of the EFT Code was issued 1 April 2001, amended 18 March 2002.

## Privacy

As Chart 6 shows, most of the reported EFT-related complaints about privacy were resolved to the satisfaction of the customer. There were just 484 of these type of complaints recorded during the period. Under-reporting of statistics has contributed to this low figure. None of the complaints were outstanding (i.e. all had been resolved).

**Chart 6: Total EFT privacy complaints by resolution**



# Appendix A: EFT Code subscribers

| |
|---|
| ABS Building Society |
| Adelaide Bank |
| American Express International Inc |
| AMP Banking |
| ANZ Banking Group |
| B&E |
| Bananacoast Community Credit Union |
| Bank Of Queensland |
| Bank Of Western Australia |
| Bendigo Bank |
| Capricornia Credit Union |
| Cashcard Australia |
| Citibank |
| Commonwealth Bank Of Australia |
| Credit Union Services Corporation (Australia) (CUSCAL)<br>(approx 156 affiliate credit unions and My Card product) |
| Dnister Ukrainian Credit Co-Operative |
| First Data International, Australia, New Zealand & South Asia |
| Gateway Credit Union |
| GE Consumer Finance |
| Heritage Building Society |
| Home Building Society |
| HSBC Bank Australia |
| Hume Building Society |
| Hunter United Employees Credit Union |
| IMB ING Bank (Australia) |
| Laiki Bank (Australia) |
| Mackay Permanent Building Society |
| Members Equity |
| National Australia Bank |
| Newcastle Permanent Building Society |
| Phoenix (NSW) Credit Union |
| Pioneer Permanent Building Society |
| Police Association Credit Co-Operative |
| Qantas Staff Credit Union |
| Queensland Country Credit Union |
| Queensland Police Credit Union |
| Queensland Professional Credit Union |
| St.George Bank |
| Suncorp |
| Territory Insurance Office |
| The Rock Building Society |
| Upper Hunter Credit Union |
| Victoria Teachers Credit Union |
| Warwick Credit Union |
| Westpac Banking Corporation |
| Wide Bay Australia |

# Appendix B: Methodology

## Monitoring instrument and procedure

The EFT Code survey monitors subscribers' compliance with the EFT Code. The survey is a self-administered instrument that relies on the honesty of subscribers in declaring whether they have conformed with various requirements set out in the Code.

The survey is divided into two main sections:

- Part A: Code of conduct checklist, which requires institutions to reply Yes, No, or N/A to questions that cover the various requirements under the EFT Code[13]; and
- Part B: Complaints statistics, which requires institutions to provide statistics about the EFT transactions and complaints they have received during the monitoring period.

The survey is presented in electronic format and delivered to subscribing institutions by email. Completed surveys must be returned in both email and hardcopy format and be accompanied by a covering letter from a senior executive of the institution that:

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

The Credit Union Services Corporation (Australia) Limited (CUSCAL) submits aggregated monitoring data to ASIC on behalf of all its affiliated credit unions. Credit unions that are not CUSCAL affiliates and all other institutions (i.e. banks, building societies and other institutions) submit individual monitoring surveys to ASIC directly.

The completed survey responses are aggregated using a customised software program and the data is then analysed by ASIC staff using a standard statistical software program. The results are presented in a report that is made available on ASIC's website(s).

## Changes to survey design

The 1 April 2003 to 31 March 2004 monitoring survey is a modified version of the survey sent for the previous period. The modifications were made in response to the poor quality of the data reported for the

[13] Comments are required for No and N/A answers.

previous period, which resulted in ASIC withholding the monitoring report for that period.

Some superficial modifications were made to Part A: Code of conduct checklist but most of the changes were made to Part B: Complaints statistics. Most notably, EFT transactions and complaints were covered under one combined Part B section rather than under separate sections for each of the following delivery channels: ATM, EFTPOS, PHONE, INTERNET, WAP and OTHER.

More generally, there have been modifications to the survey design since 2002. These, along with more minor alterations to the survey, may have affected the comparability of year-by-year results.

## Data quality

### Part A: Code of conduct checklist

Ten EFT Code subscribers reported full compliance with every clause of the Code. However due to many instances of overlap between the treatment of No and N/A in the responses to the survey by institutions, sometimes No did not mean no, but rather N/A (upon clarification of actual No responses with comments made). Where comments were not made it was not possible to separate these and so there is uncertainty about this result.

An aggregated comment was provided by the 139 *CUSCAL credit unions* in the sample, which was 90% of all credit unions in the sample (154 credit unions) and 75% of the total sample (185 respondents). In many instances no comment was provided on behalf of *CUSCAL credit unions*.

Three institutions answered N/A to most of the questions in the survey. One *other institution* had a role as a third party service provider and did not own any devices or have cardholders in its own right (as these were the responsibility of their clients) - 98% of its responses were N/A. The remaining *other institution* was not an account institution and 79% of its responses were N/A. The third was an *other bank* that only issued cards and 65% of its responses were N/A.

### Part B: Complaints statistics

In the past, some institutions have had difficulty providing some of the required complaints information. Institutions found it especially difficult to disaggregate their complaints data by delivery channel (i.e. splitting transactions and complaints by ATM, EFTPOS, Internet, Phone and WAP) following the revised EFT Code of 1 April 2002. ASIC modified the subsequent monitoring survey in order to simplify data collection. The results of this modified survey are those provided in this report.

Despite the modifications, data integrity remained a problem during this reporting period. Due to the data shortfalls, in particular a high number of part-completed statistics, this period's transactions and complaints data are most likely an underestimation of actual EFT transactions and complaints. Where possible, the researchers have qualified incomplete samples in the corresponding table notes. In extreme cases, where there was widespread under-reporting, this data has been omitted from the report.

# Appendix C: EFT Code Monitoring Survey questions (Part A – Checklist)

| REF # | EFT Code monitoring question |
|---|---|
| **Part A.1** | **ELECTRONIC FUNDS TRANSFERS INVOLVING ELECTRONIC ACCESS TO ACCOUNTS:** |
| | **Availability and disclosure of Terms and Conditions** |
| 1 | Have you developed Terms and Conditions of Use documents that reflect the requirements of the Code as revised in 2001? |
| 2 | Do the Terms and Conditions include a warranty that the requirements of the Code will be complied with? |
| 3(a) | Have you provided copies of the Terms and Conditions to account holders: - before or at the time of initial use of the access method? |
| 3(b) | Have you provided copies of the Terms and Conditions to account holders: - on request? |
| 4 | Have you publicised the availability of Terms and Conditions? |
| 4(a) | Did you publicise the availability of the Terms and Conditions: - verbally at point of sale |
| 4(b) | Did you publicise the availability of the Terms and Conditions: - in product documentation |
| 4(c) | Did you publicise the availability of the Terms and Conditions: - in product advertisement |
| 4(d) | Did you publicise the availability of the Terms and Conditions: - other - please provide explanation |
| 5(a) | Before access methods were first used, did you provide information to users: - about any separate charges for the issue or use of an access method? |
| 5(b) | Before access methods were first used, did you provide information to users: - on the nature of any restrictions imposed by you on the use of the access method (including any periodic transaction limits)? |
| 5(c) | Before access methods were first used, did you provide information to users: - about the fact that merchants or other institutions may impose additional restrictions? |
| 5(d) | Before access methods were first used, did you provide information to users: - about the types of transactions that may be made, and accounts that may be accessed, with the access method? |
| 5(e) | Describing any credit facility that can be accessed by the user through electronic equipment using the access method? |
| 5(f) | Before access methods were first used, did you provide information to users: - explaining the procedure for reporting the loss, theft or unauthorised use of a device or of breach of security of a code? |
| 5(g) | Before access methods were first used, did you provide information to users: - providing a telephone number or other means to report loss, theft or unauthorised use of an access method outside business hours? |
| 5(h) | Before access methods were first used, did you provide information to users: - explaining how users can activate complaint investigation and resolution processes? |
| | **Changing the Terms and Conditions of use** |
| 6 | Did you make changes to the Terms and Conditions in the current survey period? |

| | |
|---|---|
| 6(a) | Did you give users at least 20 days written notice of any changes to your Terms and Conditions which: - imposed or increased charges relating solely to the use of an access method, or the issue of an additional or replacement access method? |
| 6(b) | Did you give users at least 20 days written notice of any changes to your Terms and Conditions which: - increase a user's liability for losses relating to EFT transactions? |
| 6(c) | Did you give users at least 20 days written notice of any changes to your Terms and Conditions which: - impose, remove or adjust a daily transaction limit or other periodic transaction limit applying to the use of an access method, an account or electronic equipment? |
| 7 | Did you give longer notice periods where required by legislation? |
| 8(a) | Did you give notice of any other changes to the Terms and Conditions: - in time to comply with any applicable legislative requirements for a particular period of notice in advance of the date the change takes effect? |
| 8(b) | Did you give notice of any other changes to the Terms and Conditions: - If there is no legislation requirement, did you give notice of any other changes to the Terms and Conditions: - in advance of the date the change takes effect? |
| 9(a) | Did you give notice of these other changes: - in the manner required by the applicable legislation |
| 9(b) | If there were no such legislative requirements, did you give notice of these other changes: - in a manner which was likely to come to the attention of as many users as possible? Please describe the method/s used in the "Comments" box. |
| 10 | Did you issue a new consolidated Terms and Conditions document to reflect the changes resulting from the 2001 revision of the EFT code and any other changes you had made? |
| 11 | If you advised users 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 might also increase their liability for unauthorised transactions? Please describe how you advised them of this increase in potential liability. |
| | **Records of EFT transactions and notice of surcharges** |
| 12 | For EFT transactions that were not conducted by voice communications, did you ensure that receipts were issued at the time of transaction, unless a user specifically elected otherwise? |
| 13(a) | Do the EFT transaction receipts referred to in question 12 contain the following information: - the amount of the transaction? |
| 13(b) | Do the EFT transaction receipts referred to in question 12 contain the following information: - the date and time (if practicable) of the transaction? |
| 13(c) | Do the EFT transaction receipts referred to in question 12 contain the following information: - the type of transaction? (Codes may only be used if they are explained on the receipt.) |
| 13(d) | Do the EFT transaction receipts referred to in question 12 contain the following information: - an indication of the account(s) being debited or credited? |
| 13(e) | Do the EFT transaction receipts referred to in question 12 contain the following information: - data that enables the account institution to identify the user and the transaction? |
| 13(f) | Do the EFT transaction receipts referred to in question 12 contain the following information: - where possible, the type and general location of any institution equipment used to make the transaction or an identifying number or symbol? |
| 13(g) | Do the EFT transaction receipts referred to in question 12 contain the following information: - in case of a funds transfer to a merchant in payment for goods or services, the name of the merchant to whom payment is made? |
| 13(h) | Do the EFT transaction receipts referred to in question 12 contain the following information: - where possible, and not compromising the privacy or security of the account holder or user, the balance remaining in the account? |

| | |
|---|---|
| 13(i) | Do the EFT transaction receipts referred to in question 12 contain the following information: - where the balance was not provided on the receipt, please describe in the "Comments" box the delivery mechanism involved and/or why providing the balance would have compromised privacy or security |
| 14(a) | For EFT transactions that were conducted by voice communications (including an automated voice response system by telephone) did you provide to users at the time of the transaction, unless a user specifically elected otherwise: – a receipt number? |
| 14(b) | For EFT transactions that were conducted by voice communications (including an automated voice response system by telephone) did you provide to users at the time of the transaction, unless a user specifically elected otherwise: - the amount of the transaction? |
| 14(c) | For EFT transactions that were conducted by voice communications (including an automated voice response system by telephone) did you provide to users at the time of the transaction, unless a user specifically elected otherwise: - the type of transaction, eg "a deposit", "withdrawal", "transfer"? |
| 14(d) | For EFT transactions that were conducted by voice communications (including an automated voice response system by telephone) did you provide to users at the time of the transaction, unless a user specifically elected otherwise: - an indication of the account(s) being debited or credited? |
| 14(e) | For EFT transactions that were conducted by voice communications (including an automated voice response system by telephone) did you provide to users at the time of the transaction, unless a user specifically elected otherwise: - in the case of a funds transfer to a merchant in payment for goods or services, the name of the merchant to whom payment was made? |
| 14(f) | For EFT transactions that were conducted by voice communications (including an automated voice response system by telephone) did you provide to users at the time of the transaction, unless a user specifically elected otherwise: - where possible, and not compromising the privacy or security of the account holder or user, the balance remaining in the account? |
| 15 | Did you comply with the obligation not to impose a charge for issuing any type of EFT receipt? |
| 16 | In circumstances where the user did not use institution equipment or an institution system, and did not communicate with you or a person acting on your behalf, and you were not able to meet your obligations to comply with clauses 4.1(a) and 4.1(b) of the Code, did you use your best endeavours to meet those obligations? |
| 17 | Did you provide account holders with a record of account activity (statement) at least every six months? |
| 18 | Did you let account holders know that they have the option to receive statements more frequently? |
| 19 | Did you tell new account holders about this option at the time the access method was first issued |
| 20 | Did you provide account statements on request? |
| 21(a) | Did statements (other than those issued outside the usual statement cycle) show, for each transaction occurring since the previous statement: - the amount of the transaction? |
| 21(b) | Did statements (other than those issued outside the usual statement cycle) show, for each transaction occurring since the previous statement: - the date the transaction was debited or credited to the account? |
| 21(c) | Did statements (other than those issued outside the usual statement cycle) show, for each transaction occurring since the previous statement - the type of transaction? |
| 21(d) | Did statements (other than those issued outside the usual statement cycle) show, for each transaction occurring since the previous statement - the receipt number or other means that will allow the entry to be reconciled with a transaction receipt? |
| 22(a) | Did statements (other than those issued outside the usual statement cycle) also show: - any charges relating solely to the use of an access method (identified as a separate item)? |
| 22(b) | Did statements (other than those issued outside the usual statement cycle) also show: - contact details for making inquiries about the account or reporting errors in the statement? |

| | |
|---|---|
| 23 | Did statements issued outside the usual statement cycle show as much of this information as possible? |
| 24(a) | Did all statements include a suggestion that all entries should be checked and any apparent error or possible unauthorised transaction be promptly reported to the account institution? |
| 24(b) | Did you comply with the Code's requirements that there be no restrictions on account holders' rights to make claims, and that there be no time limits for account holders to detect errors or unauthorised transactions? |
| 25 | Did you, at least every 12 months, include on or with account statements a clear prominent and self-contained statement summarising access method security guidelines? |
| 26 | Were the access method security guidelines referred to in question 25 consistent with clause 5 of the Code and compliant with clause 5.8(b)? |
| 27 | Did you include, in your agreements with persons who make electronic equipment available to users for EFT transactions, a requirement that the amount of any fee to be paid directly by the user to the provider of the electronic equipment for the use of its electronic equipment, will be disclosed to the user at a time which enables them to cancel the transaction without cost? |
| | **Liability for unauthorised transactions** |
| 28(a) | If, after the adoption of the revised code, you have placed restrictions on the selection of codes by users that involve a recognisable part of the user's name or a numeric code which represents the user's birth date, did you warn users of the consequences of selecting such codes? Please describe in the "Comments" box how you deliver such warnings. |
| 28(b) | Did you provide an effective and convenient means by which users can notify a lost or stolen device or unauthorised use of a device or breach of a security code? Please describe in the "Comments" box |
| 29(a) | Do you have procedures for acknowledging users' notifications, (including those made be telephone), of the loss, theft or unauthorised use or a devise, or breach of security of a code? |
| 29(b) | Where you resolved a credit/charge card complaint in whole or in part under the EFT code, did you ensure that the amount of liability the account holder would have was not greater than it would have been if the complaint was resolved under the rules of the card scheme? |
| | **Deposits to accounts by funds transfers** |
| 30 | In circumstances where there was a discrepancy between the amount recorded by the electronic equipment or access method as having been deposited and the amount recorded by the account institution as having been received, did you notify the account holder of the difference as soon as possible? |
| 30(a) | When notifying the account holder of the discrepancy (outlined in question 30) did you advise them of the actual amount that was credited to the nominated account? |
| | **Networking Arrangements** |
| 30(b) | Do you have procedures in place to ensure that users are not required to raise their complaints or disputes in relation to the shared EFT system with another party to the shared system? |
| | **Audit trails** |
| 31 | Did you ensure that your EFT transaction systems generate sufficient records to enable transactions to be traced, checked and where an error has occurred, to be identified and corrected? |
| | **Compliant investigation and resolution procedures** |
| 32 | Have you established internal complaint handling procedures that comply with AS4269-1995 or any other industry dispute resolution standard or guideline which ASIC has declared to apply to this clause? |
| 33 | Did you provide information about the procedures for lodging complaints in your Terms and Conditions, on request, and in your general documentation? |

| | |
|---|---|
| 34 | In the case of complaints lodged and not immediately settled to the satisfaction of both you and the user, did you advise the user, in writing, of the procedures for lodging a complaint? |
| 35 | If you answered 'No' to question 34, was it because clause 10.13 of the Code applied? |
| 36 | Do your dispute resolutions procedures require you to make a decision in relation to a complaint based on all relevant established facts and not on inferences unsupported by evidence? |
| 37 | In circumstances where a user raised a complaint about the authorisation of a transaction, did you make reasonable efforts to obtain from the user the information in the schedule to the Code where the information was available and relevant? |
| 38 | Where a user raised a complaint about the authorisation or a transaction or a system or equipment malfunction, did you investigate whether there was any system or equipment malfunction at the time of the transaction? |
| 39 | Has it been the practice that, within 21 days of receipt of a complaint, you either complete the investigation and advise the user, in writing, of the outcome of the investigation; or advise the user in writing of the need for more time to complete the investigation? |
| 40(a) | Except where exceptional circumstances applied, did you complete your investigations within 45 days of receipt of the complaint? |
| 40(b) | What was the average number of days taken to resolve a complaint?<br>provide response in the "Comments" box. (Please note: you will need to tick Yes to move on to the next question) |
| 41 | If you answered 'No' to questions 39 or 40(a), was it because clause 10.13 of the Code applied? |
| 42(a) | Where an investigation could not be resolved within 45 days, did you (unless you were waiting for a response from the user that the user knew about): - inform the user of the reasons for the delay? |
| 42(b) | Where an investigation could not be resolved within 45 days, did you (unless you were waiting for a response from the user that the user knew about): - provide the user with monthly updates on progress with the complaint? |
| 42(c) | Where an investigation could not be resolved within 45 days, did you (unless you were waiting for a response from the user that the user knew about): - specify a date when a decision can be reasonably expected? |
| 43 | Did you receive any complaints concerning credit or charge cards in the survey period? |
| 43(a) | Where you decided to resolve a complaint concerning a credit card account or a charge card account under the rules of the credit card or charge card scheme did you: - apply the time limits of the scheme instead of those in sub-clause 10.5? |
| 43(b) | Where you decided to resolve a complaint concerning a credit card account or a charge card account under the rules of the credit card or charge card scheme did you: - modify the application of sub-clause 10.6 to the complaint by replacing "45 days" with "60 days" and "monthly updates" with "updates once every two months"? |
| 43(c) | Where you decided to resolve a complaint concerning a credit card account or a charge card account under the rules of the credit card or charge card scheme did you: - inform the user in writing of the time limits and when a decision could reasonably be expected? |
| 43(d) | Where you decided to resolve a complaint concerning a credit card account or a charge card account under the rules of the credit card or charge card scheme did you: - suspend the account holder's obligation to pay any amount that is the subject of the complaint and any credit and other charges related to that amount until the complaint is resolved, and inform the account holder of the suspension? |
| 44 | This question applies only if you are a member of an external dispute resolution scheme that provides that a complaint can be referred to it if a decision is not made by the account institution within a specified time period. Did you inform the account holder of the right to lodge a complaint with the scheme within 5 business days of the relevant time period expiring? |

| | |
|---|---|
| 45(a) | When you completed an investigation of a complaint, did you promptly inform the user of: - the outcome of the investigation? |
| 45(b) | When you completed an investigation of a complaint, did you promptly inform the user of: - the reasons for the outcome including references to relevant clauses of the Code? |
| 46(a) | Except where the complaint has been resolved completely in favour of the user, did you: - inform the user of any further action that the user can take? |
| 46(b) | Except where the complaint has been resolved completely in favour of the user, did you: - provide the contact details for any relevant external dispute resolution body that you belong to? |
| 46(c) | Except where the complaint has been resolved completely in favour of the user, did you: - provide the contact details for the Consumer Affairs agency and Small claims courts/tribunals in the consumer's jurisdiction if you do not belong to an external dispute resolution body? |
| 47(a) | Where, as a result of an investigation, you found you were liable, did your procedures require you to, where appropriate: - adjust the account holder's account forthwith (including any appropriate adjustments for interest and/or charges)? |
| 47(b) | Where, as a result of an investigation, you found you were liable, did your procedures require you to, where appropriate: - notify the account holder of the adjustment? |
| 48(a) | If, as a result of investigations, account holders have been held liable for at least part of any amount of a transaction in dispute, did you: - make available copies of any documents or other evidence relevant to the outcome of its investigation, including information from any relevant logs or audit trails? |
| 48(b) | If, as a result of investigations, account holders have been held liable for at least part of any amount of a transaction in dispute, did you: - advise the account holder whether there was any system or equipment malfunction at the time of the transaction? |
| 49 | If you answered 'No' to question 48(b), was it because clause 10.13 of the Code applied? |
| **Part A.2** | **RULES FOR CONSUMER STORED VALUE FACILITIES AND STORED VALUE TRANSACTIONS** |
| | **Availability and disclosure of information and Terms and Conditions to stored value facilities** |
| 50 | Does your institution offer stored value facilities or transactions?<br>Please name and describe in the "Comments" box. |
| 51 | Have you developed Terms and Conditions for stored value facilities that reflect the requirements of the Code? |
| 52 | Do the Terms and Conditions include a warranty that the requirements of the Code will be complied with? |
| 53(a) | Have you provided Copies of the Terms and Conditions to users at the time of first providing a stored value facility to a user? |
| 53(a) | Have you provided Copies of the Terms and Conditions to users at the time of first providing a stored value facility to a user? |
| 53(b) | If it is not practical to provide Copies of the Terms and Conditions to users, have you provided a summary of the main rights and responsibilities in the Terms and Conditions? |
| 54 | If you provided only a summary of the Terms and Conditions, did you also give a notice of where the user may obtain a copy of the Terms and Conditions? |
| 55 | Have you provided copies of the Terms and Conditions on request? |
| 56 | Have you publicised the availability of Terms and Conditions? |
| 57(a) | Before a stored value facility is used for the first time, did you provide the user with either full or summary information about: - any charges (imposed or controlled by you) for the issue of a stored value facility, or the issue, transfer, loading or unloading of stored value? |

| | |
|---|---|
| 57(b) | Before a stored value facility is used for the first time, did you provide the user with either full or summary information about: - any relevant period or date (if determinable at the time of issue) after which the stored value facility or stored value will not be usable? |
| 57(c) | Before a stored value facility is used for the first time, did you provide the user with either full or summary information about: - the users rights and the procedure to be followed by the user in relation to exchanging stored value for money or for replacement stored value? |
| 57(d) | Before a stored value facility is used for the first time, did you provide the user with either full or summary information about: - any procedure for reporting a malfunction or error in the operation of a stored value facility or of stored value controlled by the facility? |
| 57(e) | Before a stored value facility is used for the first time, did you provide the user with either full or summary information about: - any circumstances where you will pay to the user some or all of the amount of lost or stolen stored value? |
| 57(f) | Before a stored value facility is used for the first time, did you provide the user with either full or summary information about: - where the user can obtain more information and the Terms and Conditions for the stored value facility? |
| 58 | If you provided only a summary of the information referred to in clause 12.3, did you provide a notice of where the user may obtain full information? |
| | **Changing the Terms and Conditions of use** |
| 59(a) | Did you make changes to the Terms and Conditions during the survey period? |
| 59(b) | Did you give users advance notification of proposed changes to the Terms and Conditions for the use of stored value facilities, (unless the changes were necessitated by an immediate need to manage, restore, or maintain the integrity or security of the system or individual accounts or stored value facilities)? |
| 60 | If you knew the identity and contact details of users, did you provide notification of changes to the Terms and Conditions of the type listed in cl 13.3 directly to users? |
| 61 | In all other cases, did you publicise the changes in a manner likely to come to the attention of as many users as possible, and which has previously been advised to users?<br>Please describe the method/s used in the "Comments" box. |
| 62(a) | Did you give users at least 20 days written notice of any changes to your Terms and Conditions which: - imposed or increased charges (imposed or controlled by you) relating solely to the use of a stored value facility, or the issue, exchange, transfer, loading and unloading of stored value? |
| 62(b) | Did you give users at least 20 days written notice of any changes to your Terms and Conditions which: - adjusted the load or value storage limits applying to the use of a stored value facility? |
| 62(c) | Did you give users at least 20 days written notice of any changes to your Terms and Conditions which: - affected the user's ability to exchange stored value, notify the loss or theft of stored value or be paid the amount of lost or stolen stored value? |
| 62(d) | Did you give users at least 20 days written notice of any changes to your Terms and Conditions which: - reduced the period (if any) during which the stored value facility or stored value controlled by the facility will be useable to make a payment? |
| 63 | If you answered 'No' to questions 62(b)or 62(c), was it because the user had specifically agreed to the change? |
| | **Record of available balance** |
| 64(a) | Have you ensured that an undamaged stored value facility enables a user to ascertain the amount of stored value available for use? |
| 64(b) | If the user cannot determine the amount of stored value for use from the facility alone, have you ensured that equipment that will reveal such value is reasonably available to the user? In the "Comments" box, please describe how such equipment is made reasonably available. |

| | |
|---|---|
| | **Rights to exchange stored value** |
| 65 | Did you allow users to exchange stored value controlled by the facility for either the equivalent amount of money or replacement stored value? |
| 66 | If the user's stored value facility or the stored value controlled by the facility was no longer able to be used to make a payment, and the amount of stored value can be determined by you, did you allow users to exchange it for the equivalent amount of money or replacement stored value? |
| 67 | Did you allow consumers to exercise the right referred to in question 66 within a period of no less than 12 months from the date that it could no longer be used? |
| 68(a) | If you refused to exchange stored value under clause 15.1, was it because you proved that: - the stored value had not been created by an authorised system participant, |
| 68(b) | If you refused to exchange stored value under clause 15.1, was it because you proved that: - a copy of the stored value had previously been exchanged for money, |
| 68(c) | If you refused to exchange stored value under clause 15.1, was it because you proved that: - the user presenting the stored value is not doing so in good faith |
| 68(d) | If you refused to exchange stored value under clause 15.1, was it because you proved that: - other? Pease provide details in the "Comments" box |
| | **Refund of lost or stolen stored value** |
| 69(a) | Can you create a reliable record of the amount of stored value controlled by a stored value facility from time to time and prevent further transfers of stored value from the facility. |
| 69(b) | Do you provide a means for a user to notify you (or someone else nominated by you) at any time of the loss or theft of the stored value facility? |
| 70 | Where a user gave you notice of the loss or theft of the stored value facility, did you pay the user the amount of stored value that you could have prevented from being transferred from the facility? |
| | **Complaint investigation and dispute resolution** |
| 71 | Do you have complaint investigation and dispute resolution procedures that comply with the clause 10 of the Code (other than clauses 10.10, 10.11, 10.12, 10.13)? |
| 72 | Have you established internal complaint handling procedures that comply with AS4269-1995 or any other industry dispute resolution standard or guideline which ASIC had declared to apply to this clause? |
| 73 | Did you provide information about the procedures for lodging complaints in your Terms and Conditions, on request, and in your general documentation? |
| 74 | In the case of complaints lodged and not immediately settled to the satisfaction of both you and the user, did you advise the user, in writing, of the procedures for lodging a complaint? |
| 75 | Do your complaints resolution procedures require you to make a decision in relation to a complaint based on all relevant established facts and not on inferences unsupported by evidence? |
| 76 | Where a user raised a complaint about the authorisation of a transaction, did you make reasonable efforts to obtain from the user the information in the schedule to the Code where available and relevant? |
| 77 | Where a user raised a complaint about the authorisation of a transaction or a system or equipment malfunction, did you investigate whether there was any system or equipment malfunction at the time of the transaction? |
| 78 | Has it been the practice that, within 21 days of receipt of a complaint, you either completed the investigation and advised the user, in writing, of the outcome of the investigation; or advised the user in writing of the need for more time to complete the investigation? |
| 79(a) | Except where exceptional circumstances applied, did you complete your investigations within 45 days of receipt of the complaint? |

| | |
|---|---|
| 79(b) | What was the average number of days taken to resolve complaints?<br>Provide response in the "Comments" box. (Please note: you will need to tick Yes to move on to the next question) |
| 80(a) | Where an investigation could not be resolved within 45 days, did you (unless you were waiting for a response from the user that the user knew about): - inform the user of the reasons for the delay? |
| 80(b) | Where an investigation could not be resolved within 45 days, did you (unless you were waiting for a response from the user that the user knew about): - provide the user with monthly updates on progress with the complaint? |
| 80(c) | Where an investigation could not be resolved within 45 days, did you (unless you were waiting for a response from the user that the user knew about): - specify a date when a decision can be reasonably expected? |
| 81 | This question applies only if you are a member of an external dispute resolution scheme that provides that a complaint can be referred to it if a decision is not made by the account institution within a specified time period. Did you inform the account holder of the right to lodge a complaint with the scheme within 5 business days of the relevant time period expiring? |
| 82(a) | When you completed your investigation of your complaint, did you promptly inform the user of: - the outcome of the investigation? |
| 82(b) | When you completed your investigation of your complaint, did you promptly inform the user of: - the reasons for the outcome including references to relevant clauses of the Code? |
| 83(a) | Except where the complaint has been resolved completely in favour of the user, did you: - inform the user of any further action that the user can take? |
| 83(b) | Except where the complaint has been resolved completely in favour of the user, did you: - provide the contact details for any relevant external dispute resolution body that you belong to? |
| **Part A.3** | **PRIVACY, ELECTRONIC COMMUNICATION, ADMINISTRATION AND REVIEW** |
| | **Privacy** |
| 84(a) | Do you have procedures in place for compliance with the National Privacy Principles in the Privacy Act 1988 Cth or with a code that has been approved and is operative under that legislation? |
| 84(b) | Has compliance with those procedures been audited or reviewed in the survey period? |
| 84(c) | Do you follow the privacy guidelines set out in cl 21.2? |
| | **Electronic communications** |
| 85 | Questions 85, 86, and 87(a & b) refer to the obligations in the Code to provide certain information in writing. They apply only if you provided this information electronically. If you provided this information electronically instead of in writing or as otherwise specified in the Code, did you obtain specific positive election from the user to provide the information electronically? Please describe in the "Comments" box how this positive election was sought? |
| 86 | Did you provide the information electronically either by electronic communication to the user's device, electronic equipment or electronic address nominated by the user or by making it available at your electronic address for retrieval by the user? |
| 87(a) | If you provided the information electronically by making it available at your electronic address, did you: - promptly tell the user by sending a message to the user's device, electronic equipment or electronic address about (i) the nature of the information and (ii) that the information is available for retrieval at the specified electronic address? |
| 87(b) | If you provided the information electronically by making it available at your electronic address, did you: - provide the user with the ability to readily retrieve the information by electronic communication (eg by providing an electronic link to the relevant information at your electronic address or the URL of your website)? |

| | |
|---|---|
| 88 | If you provided information electronically to users, did you also provide users with information about their rights to vary their nominated device, electronic equipment, or electronic address, or terminate their agreement to have information provided electronically? |
| 89 | Did you provide a paper copy of information on request by a user within 6 months of the user's receipt of the same information electronically? |
| **Part A.4** | **INFORMATION ON STAFF TRAINING:** |
| | **Training Initiatives** |
| 90 | Please indicate if the following method is utilised by your institution in EFT staff training: - Procedures Manual detailing EFT requirements available to all relevant staff |
| 91 | Please indicate if the following method is utilised by your institution in EFT staff training: - On the Job Training: passive |
| 92 | Please indicate if the following method is utilised by your institution in EFT staff training: - On the Job Training: video |
| 93 | Please indicate if the following method is utilised by your institution in EFT staff training: - On the Job Training: active (e.g. team meeting) |
| 94 | Please indicate if the following method is utilised by your institution in EFT staff training: - On the Job Training: testing |
| 95 | Please indicate if the following method is utilised by your institution in EFT staff training: External Training |
| 96 | Please indicate if the following method is utilised by your institution in EFT staff training: - Resource Material Check-List: special handout |
| 97 | Please indicate if the following method is utilised by your institution in EFT staff training: - Resource Material Check-List: video |
| 98 | Please indicate if the following method is utilised by your institution in EFT staff training: - Resource Material Check-List: computer-based training |
| 99 | Please indicate if the following method is utilised by your institution in EFT staff training: - Other (please specify) |

# Further information

## Information about the EFT Code

**Download info from ASIC's consumer web site FIDO:**
http://www.fido.gov.au/codes

or

**Download info from the ASIC web site:**
http://www.asic.gov.au/codes

or

**You can also get a copy of Your Guide to the EFT Code from:**
ASIC Infoline on 1300 300 630