ABIO Special Bulletin on Electronic Commerce:
Emerging Issues in Electronic Banking Disputes

Bulletin No 35

Introduction

Electronic commerce in the financial services context includes online transactions, telephone banking and electronic funds transfer.

The ABIO accepts disputes about electronic commerce, including disputes arising out of online banking or online transactions, within our Terms of Reference. The ABIO is also the principal dispute resolution scheme for disputes under the EFT Code, which in its revised form covers online and telephone transactions.

At the outset it is important to state that the Bulletin is focussed on transactions that have given rise to disputes. It is not possible at this stage to say how the level of disputes about, for example, online banking compares to disputes about offline banking. The case studies, as with all ABIO case studies, ought to be put in the context of the vast number of transactions that take place without problems.

In addition, the categories of problems that may arise in electronic commerce, and the legal principles that apply to them, are essentially the same as those that may arise offline – a payment may go astray, an unauthorised person may operate the account or it may be operated contrary to mandate, the bank may make an error in the recording or the input of data. The way in which the problem may manifest itself, and the speed at which an error occurs, may be the result of particular features of the online environment but the problem itself is usually one that may equally occur offline.

In this Bulletin

- We discuss some emerging issues in the disputes this office is receiving about electronic commerce;
- We include some case studies which specifically focus on online banking disputes; and
- We append a commentary on the revised EFT Code which summarises the obligations imposed on account institutions by the Code, focussing on investigation obligations and the approach that will be taken by the Banking Ombudsman when considering disputes.

OMBUDSMAN

BULLETIN

The Australian
Banking Industry
Ombudsman Limited
GPO Box 3A
Melbourne 3001
Tel: 1300 780 808
Fax: (03) 9613 7345

A.B.N. 48 050 070 034

Emerging Issues in Electronic Commerce Disputes

As the case studies show, when things go wrong with electronic transactions, human error is just as likely as system malfunction to be the cause, whether it be customer error or bank officer error. A customer should certainly take no less care when using online banking as when filling out deposit and withdrawal slips or writing cheques. Likewise a bank officer should take the same care when entering data or setting up online or telephone access for a customer as would be taken in the offline environment.

The online environment does however have some features which warrant extra care, foremost of which is speed, which may in turn affect the ability to retrieve mistakes. In addition, bank staff need to keep in mind system features when giving information to customers and when taking or implementing customer instructions and banks should ensure that system features are reflected in the disclosure of information to customers.

Operating authorities and electronic banking

Mandate

The concept of mandate is fundamental to the legal obligations of a bank to its customer. With certain exceptions a bank must follow its customer's instructions as to payment of funds out of the customer's account. Those instructions will include who is authorised to operate the account. In the case of joint accounts, it is usual to express the operating instructions as 'either to sign' or 'both to sign' – the latter signifying that two signatures are required on cheques, withdrawal slips or other withdrawal instructions, such as redraw instructions for a home loan. Likewise the operating instructions for business accounts will include authorised signatories and whether one or, more usually, two are required to authorise transactions.

Insufficient authorisation

This office has received disputes about payments being made out of an account contrary to mandate in the sense that two persons are required to authorise a withdrawal from the account and only one has done so. This is not unknown in the offline environment and the law is clear – subject to certain defences and counterclaims, a bank which pays money out of an account contrary to mandate must reinstate the account.

System features and authorisation principles

An emerging issue in online and telephone banking, however, is that particular systems may not be able to accommodate a 'both to authorise' instruction, and may only have provision for one password to be entered. This may be so even where explicit instructions have been given to the contrary.

This will have repercussions where, for example, on a joint home loan or a line of credit the borrowers have given instructions that both must authorise redraws but the system allows only one to authorise a redraw via telephone or online banking. In some cases, such as where the borrowers have separated, the system deficiency, if this is the reason, will result in considerable loss for the other party and corresponding liability for the bank. Apart from the application of principles of mandate, a representation is made in accepting the instructions that they can and will be acted on. It also raises a disclosure issue – are joint account and business customers adequately informed that transactions will be allowed on one person's electronic authorisation?

Case study 1 – Bookkeeper unexpectedly empowered

C, a small business, had a policy of requiring all payments to be authorised by two people. C's bank advised their bookkeeper that C now had to authorise payments of salary electronically. A bank officer came to the office, showed C's bookkeeper how to do it, gave her a password and said 'you can transfer money to anybody'. There was no provision to allow two people to enter a password.

After a complaint to the bank, an arrangement was reached and instructions given that the payroll had to be authorised by a fax signed by two people. No loss was suffered.

Online transfers to wrong account number

Case Study 2 – Wrong person paid

D made two electronic deposits via online banking. She intended to make them to the accounts of an employee and completed the name of the account, the account number and the payment amount online. When the employee advised her that he had not received his wages, she discovered that, in error, she had transmitted the funds to an incorrect account number including an incorrect BSB number.

When she called the recipient bank, it advised her that as the name she had provided did not match the account number there should be no problem in having the funds returned and her bank confirmed that this was the case and requested the return of the funds on her behalf. After some delay however the recipient bank advised that it had been unsuccessful in contacting the person into whose account the funds had gone. It relied on industry rules, namely the Bulk Electronic Clearing System (BECS) Procedures of the Australian Payment Clearing Association Limited (APCA) to the effect that it was entitled to rely solely on account number details, regardless of whether any account name details were provided, and was not liable either to D or to her bank [clause 4.18]. In addition it relied on the fact that the BECS Procedures state that the recipient bank is not obliged to check whether the account number details are correct.

This office is in the course of considering its approach to the situation described in the case study but some comments in relation to law and good practice can be made, and feedback is welcome on the issues raised.

<u>Can the BECS rules exclude liability to the sender of a payment?</u>

The BECS Procedures [clause 4.18 and 4.19] provide that if the recipient bank has acted in accordance with the account number details provided by the sending bank but the amount has been credited to the wrong account, liability, if any, is the responsibility of the sending bank. The procedures, however, are contractual arrangements made between industry participants, including banks, and bank customers are not parties to them. Any exclusion of liability to the sender of the payment, contained in the procedures, would probably not therefore operate in law to prevent a claim being made by the sender against the recipient bank (although see the discussion on *Riedell's* case on page 8). The procedures might, however, operate to require the sender bank to indemnify the recipient bank in respect of any compensation the recipient bank had to pay to the sender.

Application of EFT Code?

In considering the effect of the BECS procedures, it is important to keep in mind the principle set out in the EFT Code that:

'Account institutions may not avoid any obligations owed to their users by reason only of the fact that they are party to a shared EFT system and that another party to the system has actually caused the failure to meet the obligations.'[clause 8.2]

What is the effect of a mismatch of account name and number?

The case study reflects the situation where the customer has made an error in keying in the account number. There is no doubt, as a practical matter, that a customer should take care in the instructions it enters. At common law, a customer has a duty to use reasonable care in executing written orders so as not to mislead the bank or facilitate forgery. Is it a breach of this duty to enter the wrong account number? Does it make a difference that the screen also provides for the entry of the account name?

There are, clearly, system efficiency reasons for relying on the account number when processing a payment and our view in the past has been that it is reasonable for a bank to rely on the account number provided by the customer. There are other principles, however, which may be relevant in determining the position at law. By seeking the account name, there is, arguably, a representation that the name is significant. In the case study, the first response of the recipient bank was that because the name and number did not match there would be no difficulty in obtaining the return of the funds and it would seem reasonable for a customer to assume that one would be checked against the other where both have been sought. So there is potentially an issue of misrepresentation as well as one of disclosure – if the industry rules are that the recipient bank will rely solely on the account number, this should be disclosed in the terms and conditions of the account. And even if this is disclosed in the terms and conditions, this may not be sufficient to avoid liability for misrepresentation/misleading conduct if it is not also disclosed on the screen at the instruction entry point.

In addition, there is a suggestion in the recent decision of the Victorian Supreme Court of Appeal in *National Australia Bank Ltd v Nemur Varity Pty Ltd* [2002] VSCA 18, that there is duty to the person on whose behalf funds are being transferred to take reasonable care to ensure that the funds are deposited to the credit of the intended beneficiary. This was not the subject of an express comment by the Court of Appeal. Rather the decision quoted without dissent a comment of the judge at first instance that it was not suggested by the bank that there was no such duty and His Honour 'could see no reason in principle or fact why such a duty did not exist' [para 32].

In that case, there was no error in the account number but the account name did not match the name on the instructions – it was not in fact the name the sender expected it to be.

What should the sender's bank and the recipient bank do if there is a mistake?

This office is sometimes asked by a bank what it should do to help the customer who has made a mistake. We also receive complaints from customers whose bank has said that it can do nothing or, in the case of recipients, that their bank has unilaterally reversed the payment out of their account without notice or consent.

In a case where the customer advises their bank that they have made a mistake in the entry of the account number, their bank and the recipient bank will be constrained by the law relating to mandate and to privacy laws. The sender and the recipient bank are not entitled unilaterally to reverse the transaction without the authority of the recipient, merely on the assertion that there has been a mistake. This would be a withdrawal on the instructions of a third party, which is a breach of mandate. Principles of privacy and confidentiality do, in many cases, prevent the recipient's bank unilaterally disclosing the name of the recipient.

There are, however, a number of steps that can be taken to minimise the chance of the recipient paying away the money in their account in the mistaken belief that they were entitled to it. Such steps might well enable the payment to be reversed with the consent of all parties, or at least put the sender in a better position to recover it. The suggested steps are also equally applicable to mistaken payments by customers offline.

The following steps, in our view, represent good practice:

- On being advised by a customer that there has been a mistake in the sending instructions, the sender's bank should notify the recipient bank immediately that an error in account number is asserted by the sender;

- On being advised of an asserted error, the recipient bank should:

    - notify its customer immediately that an error in account number is asserted (to minimise inadvertent change of position);
    - seek the recipient's consent to a reversal; and
    - in the event that the recipients asserts that he or she is entitled to the payment, seek the recipient's consent to disclosure of the recipient's name and details to the sender's bank and the sender.

The recipient may well be justified in refusing to consent to a reversal, for example, where they are in fact the intended recipient or where, in good faith, they have changed their position because of late notice of the error. A recipient who asserts that they are the intended beneficiary should however have no problem in consenting to the disclosure of at least their name to the sender. As a matter of logic, a recipient who is the intended beneficiary of a payment will have a pre-existing relationship with the sender - they must have given the sender the account name and details – and ought to have no objection to the disclosure, even if there is now a dispute between them.

If the recipient does not consent to the disclosure of the account name, what more can or should the recipient's bank do? If it is in its legal interests to disclose the account name, then under principles of confidentiality (the Tournier duty, after the case of that name) the bank may disclose the account name and details. If it is required by court order to do so then of course it must. But in the absence of a court order or process such as discovery, and in the absence of liability for breach of duty or conversion there is little more that either bank can or should do. The above

steps, however, will at least avoid an inadvertent change of position by the recipient and may well assist in obtaining the recovery of a genuinely mistaken payment.

Access to third party accounts

Case study 3 – Someone else's account on the screen

D began Internet banking and was given a client number and password. When he logged on with his client number and password he discovered that another person's account was displayed. He called the bank and was advised that he had been given an incorrect number however the bank was not able to tell him why he was able to use his password to access the other party's account. D sought an undertaking from the bank that it would advise the third party to change his or her password.

In response the bank said that what had occurred was a result of human error – an incorrect linkage of D's accounts with that of the third party. It said that it had issued new account numbers to D and the third party affected and was reviewing the application process to establish ways of eliminating similar errors in the future.

D accepted the bank's explanation and did not continue with the dispute. D had suffered no loss personally but had correctly pointed out that the third party's privacy had been breached.

Case study 4 – An unexpected hazard

D registered for telephone and Internet banking. Due to an error in linking accounts, her employer's staff welfare account, of which she was one of two signatories, was linked to her new account. D made two telephone banking transfers from the account identified as account no 1, which she thought was the new account. In fact, the withdrawal was processed from the staff welfare account. The employer discovered this first, did not accept D's explanation that it was a mistake and dismissed her. When D raised the matter with the bank its branch staff acknowledged there had been an error and promised to contact her employer and explain. For whatever reason, however, no contact was made.

At the time D brought the dispute to the ABIO, she had obtained employment but on a half time contract basis and had had an initial period of 3 month's unemployment.

Soon after the ABIO sent the letter of dispute to the bank it made contact with the disputant and with the disputant's former employer. A settlement agreement was reached to the disputant's satisfaction. At the same time the disputant made the decision to take proceedings for unfair dismissal.

Online impersonation

This office has for some time considered disputes from customers who allege that an EFT transaction, although carried out with their card and PIN, was not authorised and that their card had been misused or stolen. Online EFT transactions may also occur without authority if the wrong doer gains access to the account holder's password. Such transactions have been covered by the EFT Code since the revised Code came into effect in April this year.

The following case was decided under the terms and conditions of the account but it is noted in the case study that, as it happens, allocation of liability under the revised EFT Code would have a similar result.

Case study 5 - Teaching your children too well

The disputant questioned the bank's decision to hold her liable for $6,452 in Internet banking transfers made by her son from her cash management account to his savings account. The funds in the cash management account were substantially provided by transfers of $5,553 from the disputant's credit card account. The son also made the credit card transfers. All the unauthorised transactions occurred over a 17-day period. The disputant explained the length of time it took her to become aware of the unauthorised transactions as being due to the fact that she was away on holiday for one week of the period.

After the dispute was lodged with the Ombudsman, the bank offered to refund $1,000, being the approximate amount of the first three unauthorised transfers to the son's account. The disputant rejected the bank's offer.

Information gained during the investigation included that:

- The disputant's secret Internet banking password was her date of birth. She said she had not disclosed her password to her son;
- The son had lived at home until three days prior to the first unauthorised transfer. Earlier that same month the disputant had helped him set up his own Internet banking facility and had suggested that he choose his date of birth as his secret password;
- The bank's transaction logs showed that there were 37 Internet banking sessions during the 17-day period. Of these, 19 sessions seemed to have been initiated by the disputant and 18 by her son;
- Although the balances of the cash management account and the credit card account were adjusted immediately a transfer was made, it took at least one business day before a transfer appeared as a line item in the list of transactions (and longer when transactions were made on a weekend); and
- The disputant rarely called up a listing of cash management account transactions, but frequently called up a listing of credit card transactions – including every day for the first seven days of the unauthorised transfers.

When it came to the allocation of liability, the Ombudsman was concerned that the disputant had encouraged her son to use his date of birth as his Internet banking password just weeks before the unauthorised transactions commenced. It seemed that by doing so she may have given him a basis for correctly guessing her own password. Ultimately, however, there was not enough information to clearly demonstrate that she had voluntarily disclosed her password to her son.

The Terms and Conditions of the Internet banking facility provided that the account holder would be liable for losses if they contributed to unauthorised use by unreasonable delay in telling the bank that their access codes had been misused lost or stolen, or become known to someone else. Because the disputant was regularly calling up lists of recent credit card transactions, the Ombudsman considered that she had received sufficient information to identify the unauthorised transfers from the credit card account to the cash management and that there had been unreasonable delay in notifying the bank that her access codes had become know to someone else.

Allowing for the delay before credit card transfers appeared as a line item in the transaction listing, the point at which unreasonable delay commenced was assessed as being from the time of the disputant's internet banking session on the fifth day of the period of unauthorised transactions. By this time, there had been two transfers totalling $880 from the disputant's account to the son's account.

The Ombudsman asked the bank to limit the disputant's liability for the first two transfers to $50 and refund $830. The Ombudsman found that the disputant was liable for the remaining transfers to the son's account totalling $5,572.

The disputed Internet banking transactions occurred prior to 1 April 2002 and were not considered under the EFT Code. If they had occurred after 1 April 2002 and been subject to the EFT Code, we consider that the allocation of liability would have been similar, except that the disputant's liability for the first two transfers would have been $150 rather than $50.

Credit card fraud and online and telephone transactions – authorisation issues for small business operators

Case study 6 - Bad call

C ran a small computer sales business and was the victim of a credit card fraud. He claimed that he sold computers to the value of some $10,000 and that the bank had charged back these transactions. He complained that the purchaser paid cash for two laptops then rang with a story that friends wanted to purchase and provided credit card details over the telephone. All but one went through.

This office has received a group of disputes from small business operators with credit card merchant facilities who have had Internet transactions charged back to them even though the system had authorised them. In each case the merchants were unable to understand how this could happen and what more they could do, other than seeking authorisation, to protect themselves against fraudulent credit card use.

This is an important issue, which is yet to be resolved and which is undoubtedly exercising the minds of those involved in addressing issues of security and certainty in electronic commerce.

For the ABIO, the first task is to establish what were the contractual arrangements between the merchant and its bank. Most, if not all, merchant agreements (agreements between a merchant with access to the credit card system and the bank that supplies the access) provide that the bank will have the right to chargeback a transaction, at its discretion, if it is disputed for any reason. The right is unqualified on its terms.

In a number of cases involving chargebacks to travel agents of the cost of Ansett tickets (not involving fraud but arising because of the failure of Ansett), this office expressed the following views about the relevant provision:

- In its operation, such a provision may be harsh on merchants, particularly where as in the cases in question, our view was that the chargeback reason referred to by the banks – 'services not rendered' was unlikely to apply, as the purchased supply from a travel agent is the supply of a valid ticket (*MacRobertson Miller Airline Services v Commissioner of State Taxation of State of Western Australia* (1975) 133 CLR 125);

- While it was arguable that the provision should be read down to be limited to chargebacks which were valid under the relevant card scheme rules, to do so would be contrary to the express provision;

- An alternative argument, that merchants, and cardholders, should be able to enforce the chargeback rules, is open but yet to be determined by the courts. It was held in *Riedell v Commercial Bank of Australia Ltd* [1931] VLR 382, referred to in *Ryan v Bank of New South Wales* [1978] VR 555 at 560, that a collecting bank's customer is entitled to the benefit of clearing house rules, in that case the right to reject a late dishonour. The clearing rules, as with the credit card scheme rules, are rules binding participants in the particular payment system, some of which are to the benefit of the participants' customers and some of which are to their detriment. Would Riedell's case apply by analogy to credit card scheme rules? Should it also include the burden of such rules? [see the discussion on page 3]

- There are cogent business efficacy reasons for the provision to be unqualified. On its terms it relieves a merchant's bank from the need to resolve what might be complex arguments

between merchants and their customers. Depending on the circumstances of the dispute, resolution might be time consuming, may require determination of issues of fact or law and may well be better suited to some form of independent dispute resolution such as a court, tribunal or online ADR service.

Access to Internet banking

Case study 7 – Eye strain online

D complained to her bank and to the ABIO that she was forced to read and accept 22 pages of terms and conditions before she could proceed to her normal banking page. She did not have a printer to print the terms and conditions and considered that being forced to read and accept this amount of legally-binding information was irresponsible. D suggested that there might be an option to view later, with perhaps an expiry date for acceptance or a requirement to accept on the third time she logged in.

In response the bank advised D that it was currently reviewing its policy on the way customers are forced to view Terms and Conditions every time it enhances the web site or if any of the terms and conditions change. It suggested that she use another computer to print the terms and conditions to review at her leisure but maintained that all new terms and conditions had to be accepted before being able to continue with Internet Banking

Case study 8 – Not enough options

D complained that he had been told before travelling overseas in March 2000 that he would only need his VISA card and access to Internet banking. He said that he was assured that he could transfer funds from his cheque account to the Visa account using Internet Banking. While overseas, although D was able to connect to the Internet banking site, he was unable to utilise the funds transfer feature. He was therefore unable to transfer funds to his VISA card and was unable to use it because it was at its limit. D was without funds for a period of days. On his return, D received a message from the Internet banking facility, stating that it was intermittently experiencing technical difficulties and apologising to customers for any inconvenience.

In its response, the bank acknowledged the difficulties that D had encountered because of his inability to access funds and the embarrassment that it had caused to him as the person responsible for organising the financial matters to do with the trip. The bank confirmed that the declined transactions on D's VISA card had not affected his credit rating.

After receiving the bank's response, D did not pursue a claim for loss.

Online terms and conditions

The issue of online communication of terms and conditions is both a technical one and a legal one.

Under the Code of Banking Practice, a bank is required to provide clearly expressed terms and conditions at the time of or before making the contract [2.1 of current Code, 10.2 of revised Code to come into effect in August 2003]. While the Code of Banking Practice provides that terms and conditions may be provided as soon as possible after the provision of the banking service where it is impracticable to do so earlier, there are contractual consequences for failing to provide terms and conditions before the service is used. These consequences are referred to in what is known in law as the 'ticket cases' - cases where the contract is a 'take it or leave it' contract (contract of

adhesion) and the issue is whether sufficient notice has been given of the terms and conditions, and sufficient opportunity given to reject them and withdraw.

Offline, copies of terms and conditions are provided at the time an account is opened, or in the case of a credit card applied for by mail, in the mail prior to the collection or sending of the credit card. In such cases, written acknowledgment of acceptance may not be required, rather under the terms and conditions, first use of the card, or first access to the account, is deemed to be acceptance.

As a technical solution to the legal problem of giving adequate and effective notice of terms and conditions, a web site will usually require the user to view and accept terms and conditions before proceeding, to ensure that the terms and conditions become part of the contract. While this is an important step, and one that is in a consumer's interests, it is difficult to make this palatable to users. It can also underline to them their inability to do anything other than accept the terms and conditions or not receive the service - terms and conditions should always be read carefully by customers but in human terms it is easier to put to one side a printed booklet of terms and conditions than it is to ignore on-screen text that refuses to leave the screen until it is accepted.

Constraints on the content of online terms and conditions and best practice

Online banking usually involves 'take it or leave it' terms and conditions. This does not mean, however, that banks are free to include any terms and conditions that they wish. Where the EFT Code applies, for example, terms and conditions must:

- Reflect the requirements of the EFT Code (of particular importance in relation to allocation of liability);
- Include a warranty that the requirements of the EFT Code will be complied with; and
- Not provide for or be effective to create liabilities and responsibilities of users that exceed those set out in the Code. [See in more detail the discussion in Topic 2 of the Appendix]

In addition, banks should ensure that their online terms and conditions do not purport to exclude non-excludable warranties as to fitness for purpose or provision of services with due care and skill, such as those in s 74 of the *Trade Practices Act* and in state Fair Trading legislation.

Section 74, for example, provides that:

> '(1) In every contract for the supply by a corporation in the course of business of services to a consumer there is an implied warranty that the services will be rendered with due care and skill and that any materials supplied in connexion with those services will be reasonably fit for the purpose for which they are supplied.'

Best practice for online business to consumer (B2C) contracts is expressed in 'Building Consumer Sovereignty in Electronic Commerce – A Best Practice Model for Business'. This is a voluntary code of best practice developed by the Australian government for B2C electronic commerce (available at www.ecommerce.treasury.gov.au). Some relevant clauses are:

- Clause 30, which provides that contractual information 'should be clear, accurate and easily accessible. It should be provided in a way that gives consumers an adequate opportunity for review before entering into the transaction and to retain a record of the transaction.'

- Clause 34: 'Business should give consumers a clear and complete text of the transaction's terms and conditions. This information should be clear enough so that the consumer can access and retain a record of that information, for example, by printing or electronic record.'

ABIO Policy and Procedures Manual

The ABIO policies and procedures manual (available at www.abio.org.au) contains the policies followed by the Ombudsman's office in relation to particular disputes that frequently arise in the financial services sector.

In most cases the policies in the manual will be equally applicable to online transactions. The following policies may, however, be of particular interest:

Cleared funds	pp 15 - 18
Direct debits	pp 54 – 57
EFT investigations	pp 81 – 104
Repayment Errors	pp 123 - 131

ABIO policy in relation to credit card disputes is set out at pp 31 – 52 of the manual. Users of the scheme should note however that pp 33 – 38 are in the process of revision. The need for revision has arisen because in the course of this office considering the group of Ansett chargeback cases, referred to at page 9 of this Bulletin, the credit card schemes refused consent to the ABIO referring to the detail of the chargeback rules in its Findings and maintained that these are confidential. Under the ABIO terms of reference (clause 6.4) such confidential information cannot be relied upon to reach a decision adverse to any party to whom confidential information is denied. This means that in our Findings we will not be able to take into account the fact that a financial institution has suffered loss because of any loss of chargeback rights under the scheme rules. [see pp 36 and 37]

Requests for electronic copies of this Bulletin and comments or feedback on the issues raised in it can be made to abio@werple.net.au

September 2002

Appendix to ABIO Special Bulletin on Electronic Commerce

Investigation of Disputes about Unauthorised EFT Transactions
In Accordance with the Revised EFT Code

This commentary does not cover all aspects of the revised EFT Code, but it summarises the obligations imposed on account institutions by the revised EFT Code and the approach that will be taken by the Banking Ombudsman when considering disputes. The revised EFT Code was issued 1 April 2001 and amended 18 March 2002. The text is available from the ASIC consumer website: www.fido.asic.gov.au

TOPIC 1
Complainant Investigation and Resolution Procedures

1.1 Gathering Relevant Information

When an account institution receives a complaint about an unauthorised EFT transaction, it is required to obtain from the user at least the information outlined in the Schedule to the Code. [Clause 10.4(b)]

Comment:
Such information includes the circumstances surrounding the loss of a device or breach of a code, how code records (if any) were kept, and details of the last valid transaction.

1.2 Decision-Making

An account institution is required to make its decision in relation to a complaint on the basis of all relevant established facts and not on the basis of inferences unsupported by evidence. [Clause 10.4(a)]

Comment:
What constitutes "relevant established fact" will vary according to the circumstances of each particular complaint. However, one over-riding principle has to be kept in mind, namely: the fact that an account has been accessed with the correct access method, while significant, will not of itself constitute proof on the balance of probability that a user has contributed to losses through fraud or contravention of Code requirements [see clause 5.5(c)].

In other words, an account institution has to have some other relevant established fact to rely on (in addition to access with correct access method) before it could determine that a user had contributed to losses and allocate full liability for unauthorised transactions to a user/account holder.

Any allocation of full liability to a user solely on the basis that account access was gained with the correct access method would constitute failure to observe the complaint investigation and resolution procedures. Such a failure could mean that a bank may be liable for part or all of the amount of the transaction(s) in dispute. [see Clause 10.12 and End Note 24]

1.3 Time Frames

Within 21 days of receipt of a complaint an account institution is required to:

- Complete the investigation and advise the user in writing about the outcome; or
- Advise the user in writing of the need for more time.

An account institution should complete its investigation within 45 days, unless there are exceptional circumstances (that may include delays caused by foreign account institutions or foreign merchants being involved in resolving the complaint). [Clause 10.5 and End Note 23]

If a complaint cannot be resolved within 45 days, an account institution must inform the user of the reasons, provide monthly updates, and specify a date when a decision could be reasonably expected. [Clause 10.6]

Where a dispute involves a credit card transaction, and an account institution exercises its rights under the rules of the card scheme, the time limits under card scheme rules apply in lieu of the 21 day/45 day limits. However, updates every 2 months must be provided if the complaint cannot be resolved within 60 days.
[Clause 10.7]

Comment:
Any failure to meet time frame requirements would mean that an account institution has failed to comply with the complaint investigation and resolution procedures. Such a failure could mean an account institution may be liable for part or all of the amount of the transaction(s) in dispute. [see Clause 10.12 and End Note 24].

1.4 Notifying Outcome of Investigation

When an account institution has completed its investigation it is required to inform the user of:

- The outcome of the investigation; and
- The reasons for the outcome including references to relevant clauses of the Code; and
- Except where the complaint is resolved completely in favour of the user, the further action the user can take – including contact details for the Banking Ombudsman. [Clause 10.9]

Comment:
Note that, under the revised EFT Code, it is no longer sufficient to give reasons for the outcome of an investigation by references to an account institution's Terms and Conditions of Use. This means that any reason for allocating liability to a user must be strictly in accordance with the liability provisions of the EFT Code.

Allocation of liability for any other reason (including non-compliance with an account institution's directions for ensuring the security of devices and/or codes, that are incorporated into terms and conditions of use) would constitute a failure to comply with the complaint investigation and resolution procedures. Such a failure could mean an account institution may be liable for part or all of the amount of the transaction(s) in dispute. [see Clause 10.12 and End Note 24]

1.5 Providing Information to Users

Where an account institution decides to hold an account holder liable for at least part of an unauthorised transaction, it is required to:

- Make available to the account holder copies of documents or other evidence relevant to the outcome of the investigation; and
- Advise the accountholder in writing whether there was any system or equipment malfunction at the time of the transaction.

[Clause 10:11]

1.6 Liability because of Failure to Observe Code Procedures

Clause 10.12 provides that, even where an account institution is not otherwise liable for losses arising from unauthorised transactions or system/equipment malfunction, the Ombudsman may determine that the account institution is liable for part or all of the amount in dispute where:

- The account institution fails to observe the complaint investigation and resolution procedures set out in clause 10 of the Code; or
- The account institution fails to determine the allocation of liability in accordance with clauses 5 or 6 of the Code; or
- The account institution fails to communicate the reasons for its determination by reference to relevant aspects of clauses 5 and 6 of the Code; and
- The account institution's failure contributed to its adverse decision on the complaint (including its initial decision), or the failure delayed the resolution of the complaint (including by contributing to an accountholder's decision to refer a complaint to the Ombudsman).

End Note 24 comments that the purpose of clause 10.12 is to provide an incentive to account institutions to implement good investigation and decision-making procedures in accordance with the Code and to compensate account holders for the effects of prejudicial decisions or delays.

Comment:

This provision of the revised Code is substantially changed from a comparable provision in the old Code. The new provision means that, even where a user has contributed to losses, the ability of an account institution to allocate full liability to the user/accountholder will be diminished by any failure to observe Code requirements.

Examples of situations in which the Ombudsman might determine that an account institution is partially or fully liable include:

- Where there is failure to observe the time frames for resolution;
- Where there is failure to collect the specified information ;
- Where liability is allocated for a reason that is not a reason set out in the Code (e.g. because of what the institution considers to be non-compliance with security directions in its terms and conditions of use, but where compliance is not a contributing factor for liability as set out in the Code);
- Where an account institution allocates liability to a user simply on the basis that the correct access method has been used, without conducting a full investigation to determine whether or not the user contributed to the losses;
- Where an account institution fails to consider all reasonable evidence before reaching its decision, including all reasonable explanations for the fact that unauthorised transactions occurred;
- Where, at the time of its initial decision, an account institution fails to inform the user/accountholder of their right to refer their complaint to the Ombudsman;
- Where an account institution fails to refer to relevant clauses of the Code in a decision about liability.

At a later date, after a reasonable number of disputes have been considered under the revised EFT Code, the Ombudsman will develop policies and procedures to indicate how he is likely to determine the amount of partial or full liability in cases where an account institution fails to observe Code requirements.

TOPIC 2
Terms and Conditions of Use

2.1 Conformity with EFT Code

Because the new EFT Code covers a number of different facilities including phone banking, Internet banking, bill payment facilities such as BPay, and electronic account access using debit and credit cards, an individual account institution may have more than one set of Terms and Conditions that are applicable to EFT transactions.

Each set of Terms and Conditions is required to:

- Reflect the requirements of the EFT code;
- Include a warranty that the requirements of the EFT Code will be complied with; and
- Not provide for or be effective to create liabilities and responsibilities of users that exceed those set out in the EFT Code

[Clause 2.1]

Comment:
The specification that Terms and Conditions of Use not provide for or be effective to create liabilities and responsibilities of users that exceed those set out in the EFT Code is a new requirement. There was no comparable clause in the old EFT Code. However, when implementing the old Code in the context of dispute resolution, the policy of the Ombudsman has been that card issuers cannot elevate a cardholder's liability above what is described in the EFT Code. Effectively, the requirement in clause 2.1 of the revised EFT Code codifies the long-standing policy of the Ombudsman in regard to the old Code.

2.2 Information to be Provided before First Use of an Access Method

Clause 2.3 provides that, before an access method is used for the first time after issue, an account institution has to ensure that it provides its user with information on a number of matters, including information about:

- Any charges for the issue or use of the access method, separate from activity charges;
- The nature of any restrictions on the use of the access method, including any daily transaction limit and other periodic transaction limits that apply to the access method, an account or electronic equipment;
- The types of transactions that might be made, and of the accounts that might be accessed with the access method;
- Any credit facility that might be accessed by the user through electronic equipment using the access method; and
- The procedure for reporting a lost or stolen device or breach of the security of a code (including how to report outside of normal business hours.

Comment:
These requirements reflect similar requirements in the old EFT Code.

2.3 Transaction Limits Applicable to an Access Method

References to a daily transaction limit and a periodic transaction limit in the revised EFT Code occur in:

- clause 2.3 – relating to disclosure in Terms and Conditions, as noted above;
- clause 3.1 – relating to modifying Terms and Conditions;
- clause 3.5 – relating to advising account holders that the removal of or increase in a transaction limit may increase account holder liability in the case of unauthorised transactions;
- clause 5.5(a) & (b) – providing that an account holder's liability for unauthorised transactions may not include that portion of the losses that exceed a daily transaction limit or a periodic transaction limit; and
- clause 5.12 – providing a discretion for the Ombudsman to reduce an account holder's liability for unauthorised transactions where the account institution has not applied a reasonable daily limit or other periodic transaction limit.

In addition, End Note 16 includes a comment that:

> "A daily transaction limit may apply to the use of an access method, an account or particular electronic equipment or a combination of these."

Comment
The linkage of the daily (or periodic) transaction limit to the access method, an account or electronic equipment (including a combination of these three factors) means that an account institution has a significant degree of flexibility in setting different transaction limits for different access methods, e.g. the daily transaction limit that applies to Internet banking may be higher than the daily transaction limit that applies to card and PIN transactions; for card and PIN transactions, the daily transaction limit may be varied according to whether the transaction is conducted at an ATM, an EFTPOS terminal, or an in-branch counter terminal. However, all transaction limits must be fully disclosed to the user.

An account institution would be able to set a high daily or periodical transaction limit for a particular access method, or have no limit at all. However, an account holder's liability may be reduced if the account institution has not applied a reasonable transaction limit – having regard to prevailing industry practice.

Where an account institution has a bill payment facility such as BPay, the access method for the bill payment facility would be the same as for other phone banking or Internet banking transactions. This suggests that the revised EFT Code would not allow an account institution to set a daily limit for (say) BPay transactions that was higher than the daily limit that applied to other phone banking transactions or other internet banking transactions.

2.4 Where No Reasonable Daily Transaction Limit Applies

Clause 5.12 introduces a discretion for an account holder's liability to be reduced where no reasonable daily or periodic transaction limit applies. Clause 5.12(a) provides that the reasonableness of a transaction limit is to be determined having regard to prevailing industry practice.

Clause 5.12(b) goes on to provide that the account institution or an external dispute resolution body may reduce an account holder's liability for an unauthorised transaction by such amount as it considers fair and reasonable, having regard to:

- Whether the means used by the account institution to verify that the relevant transaction was authorised by the user adequately protected the account holder from losses in the absence of a reasonable transaction limit; and
- Where the unauthorised transaction was a funds transfer that drew on a line of credit, whether the account institution took reasonable steps to warn the account holder of the risk of the access method being used to make such unauthorised transactions.

Comment:
Before exercising a discretion to reduce an account holder's liability under clause 5.12, the Ombudsman would have regard to all the circumstances of a particular case. When assessing the reasonableness of a transaction limit, the Ombudsman would take into account the advice of his Banking Adviser about prevailing industry practice.

When assessing whether the means used by the account institution to verify that a transaction was authorised by the account holder adequately protected the account holder from loss in the absence of a reasonable transaction limit, the Ombudsman would take into account such factors as:

- the procedures set down by the account institution;
- the extent to which it could be verified that staff complied with those procedures; and
- whether a higher limit was accompanied by more stringent means than usual to verify that it was the account holder who authorised the transaction.

In the case of high-limit or no-limit card and PIN transactions at an in-branch counter terminal, the Ombudsman would take into account whether the account institution took additional steps to verify the identity and authorisation of the account holder or user, apart from mere entry of the correct PIN. If an account institution did not have additional security checks in place for such in-branch transactions, the Ombudsman might conclude that it was not reasonable to have a higher limit than that which applied to ATM/EFTPOS transactions.

When assessing whether an account institution had taken reasonable steps to warn an account holder about the risk of unauthorised access to a line of credit account, at the time of making the line of credit accessible by the access method, the Ombudsman would take into account such factors as:

- The Terms and Conditions of use for the access method, including whether the risk was clearly stated in plain English in a prominent position;
- The standard operating procedures governing the information to be given by a staff member to an account holder before the line of credit was linked to the access method; and
- Whether a warning of the risk was actually given to the account holder by a staff member at the time the line of credit was made accessible by the access method, to the extent that the scope of such a warning could be ascertained and that there was mutual agreement by the account institution and the account holder about the nature and content of the warning. Because the Ombudsman has no power to examine parties to a dispute under oath, it might be difficult or impossible for him to determine the scope of a warning if such mutual agreement did not exist.

2.5 No Time Limits for Detecting Errors or Unauthorised Transactions

Clause 4.4 of the revised EFT Code provides that:

- Account institutions will have a suggestion on account statements that account holders check statement entries and promptly report any apparent errors or unauthorised transactions; and
- Account institutions will not seek to restrict or deny account holders their rights to make claims, or attempt to impose time limits on users to detect errors or unauthorised transactions.

Comment
Clause 4.4 is carried over from a similar clause in the existing EFT Code. Thus, there is no change to current procedures re access by card and PIN.
However, account institutions will need to ensure that there is no limitation on time limits in their Terms and Conditions for other facilities such as telephone banking and internet banking. Clause 4.4 is likely to have an impact on the Terms and Conditions for credit card facilities. Although credit card transactions authorised by signature are excluded from the new EFT Code [see clause 1.5(c)], some other credit card transactions (in addition to ATM cash advances) will come under the new Code – such as purchase transactions initiated by quoting card number and expiry date over the phone or internet.

For credit card transactions covered by the revised EFT Code, clause 4.4 will require an account institution to accept notification of unauthorised transactions at any time. This will mean that an account institution may not allocate liability for unauthorised EFT transactions to a credit card holder only on the basis that they failed to report an unauthorised transaction within the time allowed for chargebacks under card scheme rules. Liability may only be allocated for the reasons set out in the EFT Code (which could include unreasonable delay in notification of the misuse, loss or theft of a device). Note that clause 10.5 of the Revised Code of Banking Practice will be read subject to these provisions in the EFT Code.

TOPIC 3
Liability for Unauthorised Transactions

3.1 No Account Holder Liability in Specified Circumstances

Clause 5.2 of the revised EFT Code carries over from a comparable clause in the existing Code and specifies certain circumstances where a cardholder will not be liable for unauthorised transactions, namely:

- Losses caused by fraudulent or negligent conduct on the part of an account institution, network participant or merchant, or their agents and employees;
- Losses relating to any component of an access method that is forged, faulty, expired or cancelled;

- Losses arising from the use of a device or code that forms part of an access method and that occurred before the user received the device or code.

  Additional comments about this principle include that:
  - in any dispute about receipt of a device or code it is to be presumed that the item was not received by the user, unless the account institution can prove otherwise;
  - account institutions can establish that a user received a device or code by obtaining an acknowledgement of receipt from the user;
  - if a device or code was sent by mail or email, the account institution is not to rely only on proof of delivery to the user's correct address as proof that the device or code was received by the user; and
  - account institutions will not have any term or condition that deems a device or code sent to the user's correct address to have been received by the user.

- Losses caused by the same transaction being incorrectly debited more than once to the same account.

Comment:
When considering complaints about unauthorised transactions, account institutions need to consider whether there has been any fraudulent or negligent conduct by system participants, including the conduct of merchants and their agents or employees. Under the comparable clause in the previous EFT Code the Ombudsman has determined that an account holder has no liability for transactions perpetrated by, say, a service station operative who observed a PIN being entered and then managed by some means to either retain or steal the card. Similar circumstances that have come to the Ombudsman's attention include fraud by taxi drivers and supermarket check-out operators.

Account institutions also need to consider whether there is any information to establish that a duplicate card may have been created by "skimming" the information from a card's magnetic strip during a legitimate transaction. While the Ombudsman himself has not yet had to consider a complaint where it was clearly established that a duplicate card had been created, he understands that there have been some instances of "skimming" in Australia where fraudulent transactions were settled by the account institutions concerned.

Any account institution that mails out devices and/or codes, such as credit or debit cards and PIN advice slips, has to accept the risk that the device or code may be intercepted by a person other than the user and that unauthorised transactions might be performed for which the account holder would not be liable.

When considering claims that a device or code had not been received by the user, the Ombudsman's policy is to consider all the circumstances of a dispute including:
- Whether the device and/or code had ever been used by the user;
- The period of time between the mailing date and the date of unauthorised access; and
- The geographical separation between the location of the mailing address and the location of the unauthorised transaction.

Some account institutions require a user to acknowledge receipt of the device or code before the access method is made operational. Provided that the acknowledgment can be substantiated (e.g. by retention of a signed acknowledgment), such institutions would be able to prove that the device or code had been received by the user in the face of a claim to the contrary.

3.2 No Account Holder Liability After Notification

Clause 5.3 of the revised EFT Code carries over from a comparable clause in the old Code. It provides that the account holder has no liability for losses that result from unauthorised transactions that occur after notification to the account institution that any device forming part of the access method has been misused, lost or stolen or that the security of codes forming part of the access method has been breached. With regard to means of notification, clause 5.9 provides that:

- An account institution will provide an effective and convenient means by which users can notify loss/unauthorised use of a device or breach of code security;
- Facilities such as telephone hot lines are to be available to users at all times, with notice by telephone being an effective notice for limitation of a user's liability; and
- Where facilities such as telephone hot lines are not available during particular periods, any losses occurring during these periods that were due to non-notification are deemed to be the liability of the account institution providing notification is made to the account institution within a reasonable time of the facility again becoming available.

Comment:

The Ombudsman's usual policy is to regard the time of notification as being the time the user phoned the account institution or spoke to a staff member at a branch, rather than the time at which a stop is recorded as having been placed on the account institution's system. This policy rarely causes practical problems because, in the experience of the Ombudsman, most account institutions do not allocate liability to the user for unauthorised transactions performed within a short time of the stop being recorded.

Some account institutions may require users to call their main telephone access number during business hours (or while their call centre is operating), and a special number during non-business hours – such as night time, weekends and public holidays. Practical problems do occur when a user is placed in a queue on a telephone system before being able to speak to an operator, or when the telephone number is engaged or does not answer.

Other problems occur when a user phones the main telephone access number after hours and receives a recorded message to ring back during business hours, without receiving a special message about how to report lost or stolen cards. The losses from unauthorised transactions may increase if a user then delays reporting the loss to the next business day.

When considering a claim that a user made an unsuccessful attempt to notify an account institution, or that a call was made prior to the stop being recorded, the Ombudsman would consider such matters as:

- The time at which a user called the account institution, to the extent that this could be verified from telephone company records;
- Call centre information provided by the account institution, including the duration of delays at the time of the call and the rate of abandoned calls;
- Whether or not the out-of-hours message on the account institution's main telephone access number included a specific number for reporting lost or stolen devices;
- The ease with which a user could look up the number for lost or stolen cards, as opposed to the account institution's main telephone access number; and
- The degree of sophistication of the user and the extent to which he or she would appreciate the urgency with which a lost or stolen card should be reported, after having heard a voice message saying to ring back in business hours.

3.3 No Account Holder Liability Where Clear that User did not Contribute

Clause 5.4 of the revised EFT Code carries over from a comparable clause in the old Code. It provides that an account holder has no liability for losses resulting from unauthorised transactions where it is clear that the user has not contributed to such losses.

3.4 Circumstances Where the Account Holder is Liable

Clauses 5.5 and 5.6 of the revised EFT Code sets out the circumstances in which an account holder will be liable for losses resulting from unauthorised transactions. Clauses 5.5 and 5.6 contain some substantially different provisions about the allocation of liability, compared to the liability clause in the old Code. Before considering the circumstances in which an account holder would be fully liable, the next part of this commentary focuses on the circumstances in which there would be limited liability.

3.5 Limited Liability

Provided that a code was required to perform the unauthorised transactions, and provided that the account institution has not proved on the balance of probabilities that the user contravened EFT Code requirements, clause 5.5(c) provides for a limited liability of $150.

Clause 5.5(c) goes on to provide that:

- In determining whether an account institution has proved on the balance of probability that a user has contributed to losses, all reasonable evidence must be considered including all reasonable explanations for the transaction occurring;
- The fact that the account has been accessed with the correct access method, while significant, will not of itself constitute proof on the balance of probability that the user contributed to losses through the user's fraud or through the user's contravention of the requirements of clause 5.6; and
- In determining whether a user has unreasonably delayed notification of the misuse, loss or theft of a device, or that the security of all the codes has been breached, the effect on the user of any charges imposed by the account institution relating to the notification or replacement of the access method must be taken into account.

Comment:
Apart from disputes where it is clear the user did not contribute to losses, in other disputes about unauthorised transactions an account holder's liability will be limited to $150 except for those cases where the account institution can prove on the balance of probabilities that the user contributed to the losses.

Limited liability only applies when a code was required to perform the unauthorised transactions. Where no code was required (e.g. credit card transactions on phone or Internet), there is either no liability at all or full liability for subsequent transactions (i.e. for transactions after the initial unauthorised transaction/s) where a user contributed to the losses arising from the subsequent transactions by unreasonably delaying notification after becoming aware of the misuse, loss or theft of a device forming part of the access method.

Because "proof on the balance of probabilities" requires an account institution to be able to rely on other "relevant established fact" in addition to account access with the correct access method, it might be expected that the majority of disputes received by account institutions about unauthorised transactions under the revised EFT Code will be resolved on the basis that the account holder's liability is limited to $150 under clause 5.5(c).

3.6 Liability for Actual Losses

Clause 5.5(a) of the revised EFT Code provides that where the account institution can prove on the balance of probabilities that the user contributed to the losses through the user's fraud or the user's contravention of the requirements in clause 5.6, the account holder is liable for the actual losses which occur before the account institution is notified that:

- a device forming part of the access method has been misused, lost or stolen; or
- the security of the codes forming part of the access method has been breached.

Even where an account holder is otherwise liable for the actual losses, the account holder is not liable for the following amounts:

- losses incurred on any one day that exceed the daily transaction limit;
- losses incurred in a period that exceed any other periodic transaction limit;
- losses incurred on any account that exceed the balance of the account (including any prearranged credit); and
- all losses incurred on any account which the account institution and the account holder had not agreed could be accessed using the access method.

The final part of clause 5.5(a) clarifies that:

- where an access method includes more than one code; and
- the account institution proves that the user contravened the requirements of clause 5.6 by voluntarily disclosing or by keeping a record of one or more codes but not all the codes in the access method;

The account holder is only liable if the account institution also proves on the balance of probabilities that the user's contravention of clause 5.6 was the dominant contributing cause of the losses.

End note 16 further clarifies that "*the dominant contributing cause of the losses*" is the cause that is more than 50% responsible for the losses when assessed together with all other contributing causes.

Comment:
The revised EFT Code places the onus on an account institution to prove on the balance of probabilities that the user contributed to the losses, before liability for actual losses can be allocated to the account holder. The requirement for the bank to prove its position is a new requirement compared to the old Code – which only stated that a cardholder would be liable if they contributed to the losses (without specifying who had to prove that the cardholder had contributed).

When considering complaints under the old Code, the Ombudsman's practice has been to conduct a parallel investigation into the circumstances of unauthorised transactions. This has meant that the Ombudsman has independently assessed whether or not a cardholder had contributed to losses, or whether it was unclear whether or not a cardholder had contributed to losses. Thus, under the old Code, the Ombudsman's determination about the allocation of liability was based on his own investigation as much as on the bank's investigation.

Because the revised Code effectively places the responsibility for an investigation on the account institution, the Ombudsman will not necessarily continue to conduct parallel investigations when considering disputes under the revised Code. Depending on the circumstances of a particular dispute, the Ombudsman may decide simply to consider all the information collected and relied on by an account institution in reaching its decision about liability. The Ombudsman would then assess whether or not he considered that the account institution had proved on the balance of probabilities that the user contributed to the losses.

In assessing whether an account institution had proved its position, the Ombudsman would take into account that the fact that the account had been accessed with the correct access method while significant, would not of itself constitute proof on the balance of probabilities that the user contributed to losses.

In other words, the Ombudsman would be likely to determine that an account institution had not proved its position if, without further investigation, it had allocated liability solely on the basis that the account had been accessed with the correct access method. Such a situation would arise,

for example, if an account institution, in response to a dispute, wrote to the account holder saying that they were liable for the unauthorised transactions "because their card and their PIN were used to access the account", without any further investigation into how the PIN had become known to a third party.

3.7 How a User Contravenes Code Requirements

The circumstances in which a user will be deemed to have contravened the requirements of the revised EFT Code are set out in clause 5.6. The requirements in the old Code are carried over (modified for the expanded access methods), and there are some new requirements as well. In summary, where an access method utilises a code or codes, a user contravenes the EFT Code where:

1. The user voluntarily discloses one or more of the codes to anyone, including a family member or friend;

2. Where the access method includes a device [e.g. a card], the user indicates one or more of the codes on the device, or keeps a record of one or more of the codes (without making any reasonable attempt to protect the security of all the code records) that are liable to loss or theft simultaneously with the device;

3. Where the access method comprises a code or codes without a device [e.g. phone banking and Internet banking], the user keeps a record of all the codes (without making any reasonable attempt to protect the security of code records) on the one article, or on several articles so that they are liable to loss or theft simultaneously;

4. The user selects a code which represents the user's birth date or a recognisable part of the user's name provided that, immediately before selection, the account institution has specifically instructed the user not to do so and warned the user of the consequences of such a selection.

   Clause 5.6 goes on to clarify that:

   - The onus is on the account institution to prove on the balance of probabilities that it gave the specific instruction and warning; and
   - The user means the actual user, taking into account the capacity of the user to understand the warning.

   End note 18 further clarifies that institutions may also technically restrict available self-selection choices by users in whatever way they wish.

5. The user acts with extreme carelessness in failing to protect the security of all the codes.

   End note 17 clarifies that *"extreme carelessness"* means a degree of carelessness which greatly exceeds what would normally be considered careless behaviour. It gives as an example somebody who stores their username and password for internet banking in a diary or personal organiser or computer (not locked with a PIN) under the heading "Internet banking codes''.

   End note 17 further clarifies that *"extreme carelessness"* does not apply to the selection of codes – which is covered by point 4 above. Endnote 17 also comments that the security of identifiers is irrelevant to liability under clause 5.5.

Comment:
It is important to note that the provisions of clause 5.6 apply only where the access method utilises a code or codes (i.e. information known to the user and/or the account institution, and which the account institution requires the user to keep secret). It is on this basis that End Note 17 refers to the security of identifiers as irrelevant to liability under clause 5.5. Another reference to the same topic is in End Note 4, which comments that the user is not liable for unauthorised transactions based on the use of an identifier without a code or a device. End Note 9 explains that an "identifier" includes an account number, card number and expiry date. (Another example of an identifier would be a customer number, though a customer number could possibly be a code if it conformed to the definition of a "code" in clause 1.5.)

Contribution to losses by self-selecting a code based on birth date or name only applies to codes selected after the revised EFT Code came into effect (i.e. on or after 1 April 2002). No liability will attach to codes selected at an earlier date and pre-existing as at 1 April 2002.

With regard to a bank being required to prove on the balance of probability that it gave the specific instruction and warning to a user at the time the user self-selected a PIN, such proof could include:

- Where the self-selection was done in-branch with the assistance of a bank officer, by providing a signed acknowledgement by the user that they had received and understood the instruction and warning; or
- Where the self-selection was done by ATM, computer terminal or phone, by demonstrating that the program guiding the user through the self-selection process included the specific instruction and warning.

3.8 Unreasonable Delay in Notification.

Under clause 5.5(b) of the revised EFT Code, an account holder will also be liable for the losses arising from unauthorised transactions where the account institution can prove on the balance of probabilities that the user contributed to losses by unreasonably delaying notification after becoming aware:

- of the misuse, loss or theft of a device forming part of the access method; or
- that the security of all the codes forming part of the access method has been breached.

The account holder is liable for the actual losses which occur between when the user became aware (or should reasonably have become aware in the case of a lost or stolen device) and when the account institution was actually notified. However, even where an account holder is otherwise liable for the actual losses, the account holder is not liable for the following amounts:

- losses incurred on any one day that exceed the daily transaction limit;
- losses incurred in a period that exceed any other periodic transaction limit;
- losses incurred on any account that exceed the balance of the account (including any prearranged credit); and
- all losses incurred on any account which the account institution and the account holder had not agreed could be accessed using the access method.

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

Comment:
The provision about unreasonable delay in notification is similar to a comparable clause in the old EFT Code.

Note that the provision only applies where a device forms part of the access method, or where the security of all the codes forming part of the access method has been breached. Effectively, there can be no liability for unreasonable delay in notification where the access method does not include a device or where the access method does not include codes.

The Ombudsman's current policies and procedures on EFT complaints, explaining his approach to the issue of unreasonable delay, are relevant to the way the he will approach complaints about unreasonable delay under the revised EFT Code (refer p.95 - 98 of the ABIO Policies and Procedures manual reproduced below).

Extract from ABIO Policies Manual: Unreasonably Delaying Notification

A cardholder must not unreasonably delay notifying the card-issuer of the misuse, loss or theft of the card or that the PIN has become known to someone else.

The Ombudsman's view is that there are two times from which delay in notifying would be measured:

Actual awareness

1. *The time at which the cardholder actually becomes aware of the misuse, loss or theft of the card, or that the PIN has become known to someone else.*

   For a cardholder to actually become aware of this fact requires more than doubt or suspicion, for example,

   - *Usually, a cardholder will need to check that a card has not been misplaced before he/she actually becomes aware that the card is lost or stolen;*

   - *Usually, a cardholder's doubts or suspicions that someone may have seen him/her enter a PIN at a terminal will not make him/her actually become aware that the PIN has become known to someone else.*

Should reasonably have been aware

2. *The time at which the cardholder should reasonably have become aware of the loss or theft of the card (note: this does not apply to misuse of the card or to the PIN becoming known to someone else).*

   This time arises when a reasonable cardholder, with the actual cardholder's pattern of card use and in the actual cardholder's circumstances at the time, would reasonably have checked on the presence of the card, either to use it or to confirm that the card was still in his/her possession in such circumstances as:

   - *Where there is evidence of theft or attempted theft which would make a reasonable person check the presence of his/her card (for example, there has been a burglary, the cardholder's office has been rifled, or there has been an attempted pick-pocketing); or*

- *When a reasonable period has elapsed since the cardholder last saw or verified the presence of the card, and it would reasonably be expected the cardholder would have looked for the card to use it by the end of that period (taking account of the actual cardholder's normal usage patterns and variations due to circumstances such as illness, or being at home, or on holiday).*

This test of when a cardholder should have checked the whereabouts of his/her card does not impose an obligation on the cardholder to regularly use the card. The test is subjective. This means that we would look at the cardholder's usual practices and his/her explanations for any variations from that practice.

It is not an unreasonable delay for the cardholder to take a reasonable time to ensure the card has not been misplaced, to search for the card, if the cardholder believes it has been lost, or to notify police or security officers before notifying the card-issuer.

Nor is it an unreasonable delay for the cardholder to notify a branch (if he/she becomes aware of the loss or theft within financial services provider hours) rather than the financial services provider' hotline. Delays in notifying the financial services provider caused by congestion on the hotline or at the branch are not unreasonable delays by the cardholder.

Delays because of doubt or suspicion

Concern has been expressed about how liability might be apportioned in the following scenario:

- *There was unauthorised access to an account using card and correct PIN;*
- *The card issuer denied the claim on the basis that the cardholder unreasonably delayed notification;*
- *The cardholder delayed contacting the financial services provider because he/she was unsure whether he/she had lost the card and did not want to unnecessarily incur the inconvenience and costs associated with obtaining a replacement card.*

In other words, if a cardholder's search was a little longer and a little more thorough than the average in order to ensure that the card really was lost or stolen and the thief used this time to access the account would the cardholder be liable?

If a cardholder takes this option then the cardholder is:

1. *Allowing a thief more time to access the account; and*
2. *Putting him/herself in a position where he/she may have to show that he/she acted reasonably in taking extra time.*

In order to test whether the time taken was reasonable, this office would ask questions to discover:

1. *Whether the cardholder had good grounds for doubting that the card had really been lost or stolen;*
2. *Whether the cardholder had previously incurred this inconvenience and cost unnecessarily;*
3. *Whether the cardholder's finances were so delicately placed that his/her decision making would be affected in this way; and*
4. *How much longer the search took as a result of this concern about those costs: 5 minutes, 3 hours, a day?*

All of these matters would be taken into account in assessing the case.

Summary

If an unauthorised transaction takes place:

- *Before the cardholder actually becomes aware or should reasonably have become aware of the loss or theft of the card under 1 or 2 above; or*
- *While the customer is reasonably:*
- *Ensuring that the card has not been misplaced;*
- *Searching for the card; or*
- *Notifying police or security officers,*

before notifying the card-issuer or making a reasonable effort to notify the card issuer,

then the cardholder does not contribute to the loss from that unauthorised transaction and is not liable on the basis he/she unreasonably delayed notification.

3.9 Reasonable Attempt to Protect the Security of Code Records

Clause 5.8(a) of the revised EFT Code clarifies that a reasonable attempt to protect the security of a code record includes either or both of:
- making any reasonable attempt to disguise the code(s) within the record; or
- taking reasonable steps to prevent unauthorised access to the code record.

End Note 20 further clarifies that reasonable steps to prevent unauthorised access may involve:
- hiding or disguising the code record among other records or in places where a code record would not be expected to be found;
- keeping a record of the code in a securely locked container; or
- preventing unauthorised access to an electronically stored record of the code.

Comment:
The Ombudsman's current policies and procedures on EFT complaints, explaining his approach to the issue of reasonable disguise of a PIN, are relevant to the way he will approach complaints about protecting security of codes under the revised Code (refer p.92ff of the ABIO Policies and Procedures manual set out below).

Extract from ABIO Policies Manual: Reasonable attempt to disguise a PIN

Reasonable attempt to disguise a PIN

A cardholder must not keep a record of the PIN with any article carried with the card or liable to loss or theft simultaneously with the card, without making any reasonable attempt to disguise the PIN.

The ACCC/Treasury EFT Code Review Taskforce in its report of March 1998 reported on page 62:

> *"The taskforce is of the view that cardholders should not be unreasonably prohibited from recording PINs, and that any interpretation of the phrase "reasonably disguised", whether in the Code or in*

individual terms and conditions, should have regard to what was reasonable in the particular circumstances".

Attempts to disguise a PIN

The Ombudsman's view is that a PIN may be disguised by:

1. *Concealing the number's identity as a PIN within the record by altering the content of the PIN.*

   For instance, by:

   - *Re-arranging the numerals; or*
   - *Substituting other numerals or symbols;*

2. *Concealing the number's identity as a PIN within the record, without altering the numerals in the PIN or their order.*

   For instance, by:

   - *Making it appear as another type of number;*
   - *Surrounding it with other numerals or symbols.*

3. *Concealing the PIN record's identity as a PIN record by placing the record in a location or context where it would not be expected to find a PIN.*

   For instance, on a piece of paper in a cookery book; or

4. *Concealing the PIN using some combination of these approaches.*

Assessing reasonableness of attempt to disguise the PIN

In assessing whether a cardholder has made a reasonable attempt to disguise the PIN, the following principles apply:

Standard of attempt

1. *The attempt to disguise the PIN does not have to be the most reasonable that could have been undertaken;*

2. *The fact that a PIN disguise failed to prevent unauthorised transactions does not make the attempt to disguise the PIN unreasonable. In all disputes about reasonable disguise, the PIN disguise will have failed. The reasonableness of a PIN disguise should be assessed apart from the fact that the disguise failed.*

The reasonable cardholder

3. *The reasonableness of the attempt to disguise should be assessed from the point of view of the reasonable cardholder.*

   The reasonable cardholder is a person:

- *Of average intelligence;*
- *Who does not have the knowledge and experience of a thief or financial institution claims officer about the strengths and weaknesses of different types of disguises;*
- *Who is aware of widely publicised warnings by the Ombudsman and/or by his/her financial services provider of unsafe methods to disguise a PIN and would not use such methods unless additional features of disguise were also used in an attempt to reasonably disguise the PIN.*

Each case to be assessed individually

4. *The Ombudsman will consider on the facts of each case whether the cardholder has made a reasonable attempt to disguise the PIN within the meaning of the EFT Code, taking account of all relevant information including:*

- *The manner of disguise of the PIN;*
- *The speed with which the account was accessed;*
- *Whether the correct PIN was used at first attempt; and*
- *Any other information surrounding the PIN in the record and the location and context of the record containing the PIN; and*

Relevance of cardissuer's educative activities

1. *In determining whether an attempt to disguise was reasonable or not, the Ombudsman will take into account any directions by the financial services provider about unreasonable forms of disguise which it has widely publicised to cardholders or which appear in its T&C.*

Educative activities

To ensure that cardholders have clear guidance on which methods of disguise could be used and which should not be used as they are more easily penetrated, card issuers should tell cardholders about these disguises in:

1. *T&C;*
2. *Writing to the cardholder;*
3. *Educational material displayed in financial services provider branches and/or at ATMs; and*
4. *Advertising campaigns.*

Easily penetrated disguises

The experience of the Ombudsman's office is that the following ways of recording a PIN are often penetrated by thieves and it is strongly suggested that cardholders do not use these ways for recording their PINs:

1. *Recording the PIN as a series of numbers with any of them marked or circled or highlighted to indicate the PIN;*

2. *Recording the PIN with surrounding information that makes it stand out from its context. For instance, a PIN recorded as a four or six digit telephone number where all the other numbers are eight digit numbers;*

3. *Recording the PIN as a string of digits in isolation from other information, unless the context of the information within the record or the context of the record itself provides adequate disguise,*

4. *Recording the PIN as a:*

   - *Birth date;*
   - *Postcode; or*
   - *Telephone number*

   without additional features of disguise.

The inclusion of a method of recording a PIN in this list does not create a presumption that an attempt to disguise a PIN using that method is always unreasonable. That is a question of fact and context in each case.

3.10 Security Guidelines versus Liability for Breach of Security of Code(s)

Clause 5.8(b) of the revised EFT Code provides that an account institution may set out guidelines in its Terms and Conditions for a facility designed to ensure the security of an access method. Any such guidelines are to be consistent with clause 5 and must:

- clearly differentiate those guidelines from the circumstances in which an account holder is liable for losses resulting from unauthorised transactions; and
- include a statement that an account holder's liability for such losses will be determined under the EFT Code rather than the guidelines.

Comment:
The provisions of clause 5.8(b) are consistent with the provision in clause 2.1 that an account institution's Terms and Conditions will not provide for or be effective to create liabilities and responsibilities of users, which exceed those set out in the EFT Code.

3.11 Credit Card Transactions by Phone and Internet

Comment:
Credit card transactions initiated by phone or Internet will be covered by the revised EFT Code. In terms of the definition of "access method", such transactions involve the use of two identifiers (card number and expiry date) given through electronic equipment (telephone or computer). The access method does not include either a device or codes. A card is a device. But when card number and expiry date are quoted by phone or Internet, it does not seem that the card or device forms part of the access method because the device itself is not used with electronic equipment to access the account.

Effectively, an account holder can never be liable for unauthorised phone and Internet credit card transactions where knowledge of the card number and expiry date was gained independently of the card itself, e.g. from a copy of a credit card voucher or from a list posted on the Internet.

There could be some account holder liability where the third party making the unauthorised transaction had gained access to the card itself in order to ascertain the card number and expiry date. Where a card was lost or stolen and an account holder unreasonably delayed notification, the account holder would be liable for the actual losses from the time that they should reasonably have become aware that the card was lost or stolen. In other words, the account holder would not be liable for initial phone or Internet credit card transactions that occurred prior to the time that they became aware (or from the time that they should reasonably have become aware) that a card was lost or stolen, but would be liable for subsequent transactions where there was unreasonable delay in notification after becoming aware.

Where a card was not lost or stolen but was misused (e.g. by a family member or friend) there is a less stringent test for determining the time from which the account holder would become liable. Where, for example, one family member used knowledge of card number and expiry date from another's family member's card to make unauthorised phone or Internet transactions, the account holder would only be liable from the time that they actually became aware of the misuse of their card and then unreasonably delayed notification of the misuse to their account institution.

No time limits can be applied to the detection of unauthorised transactions involving phone and Internet credit card use because of the provisions of clause 4.4, which provides that account institutions will not restrict the right to make claims or impose time limits on the detection of unauthorised transactions.

Furthermore, liability could not be allocated to the account holder on the basis that unauthorised transactions were reported after chargeback time limits had expired because of the provisions of clause 2.1, which provides that terms and conditions will not provide for or be effective to create liabilities and responsibilities of users which exceed those set out in the Code.

TOPIC 4
Commencement Date of New EFT Code

4.1 Administrative provisions re commencement

Clause 23.1 provides that the Code shall become binding on code subscribers on 1 April 2002 (with the exception of the clause about notice of surcharges for using foreign equipment, which becomes binding on 1 April 2003).

End note 45 comments that the old provisions of the Code cease to operate from 1 April 2002.

Comment:
Where the unauthorised transactions that are the subject of an EFT dispute occurred prior to 1 April 2002, the Ombudsman will continue to consider such disputes under the provisions of the old EFT Code.

Where the unauthorised transactions occurred on or after 1 April 2002, or are part of a sequence of transactions that commenced prior to 1 April but finished on or after 1 April 2002, the Ombudsman will consider the dispute under the provisions of the revised EFT Code.