FINANCIAL OMBUDSMAN SERVICE

Banking & Finance
Policies and Procedures Manual (Extract)

This extract comprises the sections of the Policies and Procedures Manual developed by the Banking & Financial Services Ombudsman which deal with:

1. Credit Card Disputes; and

2. Electronic Funds Transfer ("EFT") Investigations

This extract has been prepared in conjunction with the release of Bulletin 59, September 2008, which deals with the impact of the EFT Code on PIN@POS transactions and MOTO transactions.

CREDIT CARD DISPUTES

This section draws together BFSO's policies and approaches to the variety of issues raised by disputants about credit card use.

Authorisation: Was the Disputed Transaction Authorised by the Account-Holder?

The central issue in a dispute about a credit card transaction being wrongly debited to an account is whether the transaction was authorised. Set out below are:

1. The explanation of why authorisation is the crucial issue to be investigated; and

2. The kinds of questions this office asks when investigating whether a transaction was authorised.

Authorisation is the Central Issue

The conditions of use for credit card accounts together with any terms implied by the law constitute the contract between the card issuer and the account-holder.

The conditions of use identify each party's entitlements and obligations, including:

- How the account can be used;
- What the disclosed credit limit is; and
- What the terms of repayment are.

In summary, if an account-holder provides the card details to a merchant over the telephone or Internet or presents the card with or without signature, the account-holder authorises the transaction.

Disputes arise when the account-holder disputes that he/she authorised the transaction debited to the card account.

The issue of contractual liability for the transaction therefore primarily turns on whether the account-holder in fact authorised the transaction. In broad terms, for the card issuer to debit the account without such authorisation would usually, on the face of it, be a breach of, or outside the contemplation of, the terms of the contract by the card issuer.

Investigating Authorisation

Therefore, in all investigations of cases of disputed transactions, this office would ask:

Q: Do the facts establish that the account-holder authorised the disputed transaction?

To determine this issue, we would ask questions such as:

Q: Did the cardholder participate in the transaction?
Q: How did the cardholder participate in the transaction?
Q: What transaction(s) did the participation authorise?

Conclusion

If the transaction was not authorised by the account-holder, then the account-holder would not be liable for the transaction unless there was a specific term of the credit card contract, which changed this fundamental relationship between the cardholder and the issuer bank.

One situation in which, even though the transaction was not authorised, nevertheless the account-holder may be liable can arise if the account-holder delayed notifying the financial services provider that he/she disputed the transaction. (For a full discussion of this possibility see page 8: "Disputing Transactions Outside Time Limit").

If the transaction was authorised by the account-holder, then the account-holder would be liable for the transaction unless liability for the transaction(s) should be set aside for some other reason.

One situation in which, even though the transaction was authorised by the account-holder, nevertheless the account-holder may not be liable can arise if the card was being used over its credit limit. This shift in liability could arise because:

- The merchant failed to obtain authorisation from the account-holder's financial services provider for the transaction; and/or

- The account-holder had been misled about the operation of the credit card limit; and/or

- The granting of credit above the approved credit card limit amounted to maladministration by the financial services provider.

Credit Cards: Chargeback

Set out below is a discussion of the inter relation of two relationships:

1. The account-holder and his/her financial services provider; and

2. The account-holder's financial services provider and other banks in the card operating scheme (such as VISA and MasterCard).

This inter relation is determined primarily by the "chargeback" arrangements which operate under the card operating scheme.

What is a "Chargeback"?

A chargeback is a right which may be exercised in certain situations by an issuer's (cardholder's) financial institution against an acquirer's (merchant's) bank. It is a right to charge back responsibility for a credit card transaction from the issuer financial institution to the acquirer bank.

There are varying requirements and time limits within which an issuer financial institution must exercise its right. The chargeback rights and requirements are identified in the operating rules of the various card schemes.

Time Limits & Chargeback Rights

There are different time limits for the exercise of different chargeback rights. The time limits are specified in the operating rules but they are not disclosed to account-holders. They may, however, be relevant to the dispute between the financial services provider and the account holder in a number of ways.

Credit card conditions of use generally warn account-holders that they need to dispute transactions immediately they receive their account statements. Problems can arise if this term is not clearly expressed in the conditions of use (For a full discussion of these issues, see page 8: "Disputing Transactions Outside Time Limit").

Relevance of Chargeback Rights

The chargeback arrangements are critical in determining:

- Will the account-holder's financial institution (and therefore the account-holder) bear the amount of the transaction? or

- Will the account-holder's financial institution be able to charge the amount of the transaction back to the merchant's bank so that the account-holder's financial institution (and therefore the account-holder) is not liable for a transaction?

The Obligation to Chargeback

There is no express contractual obligation imposed on an issuer financial institution to exercise chargeback rights on behalf of an account-holder. However, industry acceptance of the custom of processing all disputed transactions as chargebacks, where a chargeback right exists, is so common that the Ombudsman has determined that it is good industry practice to chargeback.

Therefore, this office's view is that if an account-holder disputes a transaction and chargeback rights exist under the relevant card scheme operating rules, the financial institution is obliged to:

1. Process all disputed transactions as chargebacks, where chargeback rights exist;

2. Take care in exercising any chargeback right. This would include using the most appropriate reason code for the chargeback, so that the account-holder's reasons are properly represented, and properly completing chargeback documentation under the relevant card scheme; and

3. Satisfy itself that the response to the chargeback, given by the merchant's bank, is a proper response to the situation.

BFSO Investigation of Chargeback

In cases of disputed transactions, this office would ask:

Q: Did the financial institution exercise its right(s) of chargeback for each of the disputed transactions?

Q: Did the financial institution use the most appropriate chargeback right available for each of the disputed transactions?

Q: Did the financial institution satisfy itself that the response it received from the acquirer bank was an appropriate and full response to the chargeback right it exercised?

Disputing Transactions Outside Time Limit

While authorisation is the key issue in determining liability for a credit card transaction, there may be certain circumstances in which liability for the transaction lies with the account-holder even though the transaction was not authorised by the account-holder. This situation can arise if the conditions of use for a credit card specify that if the account-holder delays notifying his/her financial institution that a transaction is unauthorised, then the account-holder may be liable for the transaction.

Credit card conditions of use & time limits

Conditions of use for credit cards usually include such a term because issuer financial institutions seek to ensure that they do not lose their chargeback rights because the right is exercised too late.

This office's view is that in order for this term in the conditions of use to operate effectively, it needs to clearly say that a failure to notify the financial institution of a dispute within a specified time may lead to the account-holder being liable for an unauthorised transaction.

However, not all financial institutions' conditions of use are clear. Some conditions of use say:

- The account-holder must notify the financial institution if a transaction is disputed: "immediately" or "promptly" or the account-holder may be liable for the unauthorised transaction; others say,

- The account-holder must notify the financial institution if a transaction is disputed "immediately" or "promptly" or within for instance, 3 months, but do not then go on to say what the consequences of failing to notify the bank of the dispute within that time may be.

BFSO approach

Set out below are this office's views on the principles to be applied when:

1. There is an undefined time limit for the fulfilment of the account-holder's obligation to notify the financial institution of a disputed transaction; and

2. The conditions of use do not specify the consequences of not complying with a deadline.

Obligation to "promptly" notify financial institution of dispute

This office's view is that if the term in the conditions of use requires the account-holder to notify the financial institution "promptly" or "within a reasonable period of time" of a disputed transaction then the obligation imposed on the account-holder is that he/she must not unreasonably delay notifying the financial institution of the dispute.

In determining whether or not there has been an unreasonable delay, we will look at the circumstances of the dispute and ask:

Q: When should the account-holder reasonably have become aware of the unauthorised transaction? and

Q: When should the account-holder reasonably have notified the financial institution?

Time limit not linked to liability

Some financial institutions' conditions of use do not specify the consequences of not complying with a deadline. In this situation:

Account-holder

An account-holder may say that he/she did not authorise the transaction and so is not liable for:

1. The amount of the transaction; and

2. Interest and fees charged by the financial institution in respect of the transaction.

Financial Institution

A financial institution may say that:

1. The time limit stated in the conditions of use for disputing transactions has expired;

2. The financial institution no longer has chargeback rights; and therefore,

3. The account-holder must bear the loss.

Analysis

Account-holder not contractually liable

In the event that the financial institution is not able to produce information demonstrating that the account-holder authorised the transaction, this office's view is that the account-holder is not contractually liable for:

1. The amount of the transaction; or
2. Interest and fees charged by the financial institution in respect of the transaction.

Account-holder's breach of contract

However, the financial institution may be prevented from obtaining the necessary information because the account-holder has delayed in disputing the transaction. If the account-holder has disputed the transaction outside the specified time limit, the account-holder has breached the contract and in so doing may have caused the financial institution loss or damage.

What is the damage to the financial institution?

This office's view is that the damage to the financial institution caused by the account-holder's breach of contract is the loss by the financial institution of its right to chargeback the transaction.

Amount of the transaction

If the account-holder had disputed the transaction within the time limit specified in the conditions of use, the financial institution could have charged back the transaction. The outcome of a chargeback would have been either:

1. The merchant's bank would have responded with information to establish that the account-holder authorised the transaction; or
2. The merchant bank would have had to accept the chargeback.

In either event, the financial institution would not have had to bear the cost of the transaction itself.

The financial institution loses both of these options because of the account-holder's breach of the credit card contract. This means the damage to the financial institution is the amount of the transaction.

Interest & fees

Because the financial institution is not able to establish that the account-holder authorised the transaction, it consequently cannot establish that it was entitled to charge interest (or fees such as foreign currency conversion fees). Therefore, the financial institution is unable to demonstrate that it has suffered loss in respect of interest and fees as a result of the account-holder's breach of contract.

Conclusion

In summary, the account-holder may be liable for the amount of the transaction but not for any consequential interest or fees.

Credit Cards: Over the Limit Use

The discussions on previous pages have focused on liability where a credit card transaction is disputed on the basis it was not authorised.

However, there are situations in which, even though the transaction was authorised, nevertheless the account-holder may not be liable. This shift in liability can arise if the card was being used over its credit limit.

Disputes Received by BFSO

Examples of the kinds of disputes we have received include:

- A merchant charging, under a car rental agreement, in excess of $10,000 to a customer with a credit card limit of $500;

- An account-holder authorising the issue of a secondary card to a family member in the belief that the card had a credit limit of $3,000 and the secondary cardholder obtaining credit to $6,000.

When Might a Financial Services Provider be Liable for Authorised Transactions?

A shift in liability for an authorised transaction from the account-holder to the financial institution could arise because:

1. The merchant failed to obtain authorisation for the transaction; and/or

2. The account-holder's financial institution gave a merchant authorisation for a transaction which exceeded the account-holder's credit limit; and/or

3. The account-holder was misled about the operation of the credit card limit; and/or

4. The granting of credit above the approved credit card limit amounted to maladministration by the financial institution.

The discussion below sets out our policy in relation to each of these scenarios.

Merchant Failed to Obtain Authorisation

We have been looking at cases where the account-holder:

1. Disputes transactions processed to his/her credit card account by a merchant; and

2. The debits by the merchant have led to the credit limit on the card being exceeded.

Floor Limits

One of the most obvious rights to chargeback arises where the transaction is above the relevant merchant's floor limit and no authorisation for the transaction has been obtained by the merchant from the account-holder's financial institution.

There may well, of course, be many transactions for which authorisation is not obtained by the merchant and the transaction is not disputed. This happens on a daily basis and causes no problem. The problem arises where the account-holder disputes the transaction and there was no authorisation obtained by the merchant.

If a transaction is disputed, we ask:

Q: Was the disputed transaction above or below the merchant's floor limit?

Below Floor Limit

If the disputed transaction was below the merchant's floor limit:

- As between the issuer and acquirer financial institutions, the disputed transaction may be a valid transaction in accordance with the card scheme's operating rules, so that there is no right of chargeback for the cardholder's financial institution;

- A financial institution should be alert to the possibility of multiple fraudulent transactions or of a merchant splitting sales to keep transactions below the floor limit.

Above Floor Limit

If the disputed transaction was above the merchant's floor limit, we ask:

Q: Was the disputed transaction properly authorised by the financial institution?

If the merchant did not obtain a proper authorisation, then the disputed transaction would not be valid under the card scheme's operating rules and the issuer financial institution should exercise its chargeback rights.

<u>Effect of this approach on merchants</u>

We consider this approach fair because:

1. The card schemes and merchant agreements instruct a merchant to obtain authorisation for a transaction above the merchant's floor limit;

2. If the merchant obtains the authorisation, then the merchant will, if no other chargeback right exists, receive payment via the card scheme for the goods or services supplied;

3. If the merchant does not obtain the authorisation then the merchant chooses to take the risk that the credit card transaction may not be valid; and

4. The merchant may have rights against the purchaser, as a merchant would have rights if a cheque was dishonoured, but for the purposes of the card schemes, the transaction may be charged back.

Transactions Over the Credit Limit Authorised by the Financial Institution

If the merchant obtained authorisation from the account-holder's bank for a disputed transaction which took the account over its credit limit:

1. We would usually conclude that the financial institution should not have authorised the transaction; and

2. We will investigate whether the account-holder has suffered a loss as a result of the incorrect authorisation.

Has the Account-Holder Suffered a Loss?

The matters we will look at to determine loss include:

Q: Did the account-holder receive a benefit as a result of the disputed transaction?

Q: Did the incorrect authorisation lead to a minor or a serious overdrawing of the credit limit?

Q: Does the account-holder's account history show frequent over the limit use of the card followed by repayments?

Q: Was the transaction payment of a debt already owed by the account-holder?

Misleading Conduct

In some cases, even though the transactions were authorised by the account-holder, the transactions may be set aside because the account-holder may have been misled about the operation of the credit card limit.

Disputes received by BFSO

Disputes we have considered in this category include where:

1. The account-holder authorised the issue of a secondary card for use by a business partner in the belief that the maximum liability she might have for the transactions of the business partner/secondary cardholder would be the credit card limit of $3,000. The secondary cardholder used the card to authorise transactions to $5,000.

2. The account-holder provided his card as security for a third party's hire of a car in the belief that as the credit limit was $2,000 and his own transactions had

led to a debit balance of $1,600, the maximum liability he might have would be $400. Transactions were posted to the account by the car hirer leading to a debit balance of $3,500.

Conditions of Use

The conditions of use for credit cards usually specify that there is a credit limit for the card above which credit will not be provided.

On the other hand most conditions of use also anticipate that an account balance may exceed its limit and provide that the amount in excess of the credit limit must be repaid immediately.

This office's view is that the reference to the possibility of exceeding the credit limit must be read within the context of the prohibition on exceeding the credit limit.

Therefore, the conditions of use may not amount to a sufficiently clear warning to an account-holder that drawings in excess of the credit limit may be allowed by the bank on the account.

The Conduct

In light of the prohibition on use of a card over its credit limit, there is a risk that an account-holder may be led into the false impression that he/she can only use the card up to, but not exceeding, the credit limit in the ordinary course.

A financial institution may engage in misleading conduct by failing to disclose any excess amount up to which it will authorise transactions, which is above the credit limit disclosed to its account-holder, leaving the account-holder under the false impression that the financial institution will not permit the account to be overdrawn as a matter of course.

Depending on the circumstances, this false impression could have serious consequences for the account-holder. In particular, serious consequences could ensue where a second card on the account has been authorised by the account-holder in reliance upon the disclosed conditions of use, which led the account-holder to believe that credit could not be accessed beyond the disclosed credit limit.

In summary, non-disclosure of any excess limit may, in particular circumstances, mislead account-holders in a way that is actionable. It would be necessary, of course, for the account-holder to establish that he/she was actually misled as a result of his/her reliance upon the financial institution's conditions of use, or other conduct. In many cases, it may be difficult for account-holders to establish the necessary reliance.

<u>BFSO investigation</u>

If a dispute raises these issues, the questions we will ask include:

Q: What was the credit limit for the card?

Q: Why did the financial institution allow the credit limit to be exceeded?

Q: Was the account-holder aware that the credit limit could be exceeded?

If the account-holder knew the credit limit could be exceeded, it is unlikely that misleading conduct leading to loss can be established.

Did the account-holder rely on the misleading conduct?

To assess this issue we will investigate the following question:

Q: If the account-holder did not know that the credit limit could be exceeded, did the account-holder rely on a perceived limitation of liability created by the existence of the credit limit?

Has the account-holder suffered a loss?

To assess this issue we will investigate the following question:

Q: If the account-holder did not know the limit could be exceeded and relied on the existence of the limit, what loss, if any, has the exceeding of the limit caused the account-holder?

Maladministration

Another circumstance in which liability for authorised transactions may shift from the account-holder to the financial institution, notwithstanding that transactions were authorised by the account-holder, is if there was maladministration by the financial institution in the provision of credit to the account-holder.

Assessing capacity to repay

As with the provision of all loans, a financial institution will assess an application for credit against its lending criteria. Using such criteria, a financial institution will calculate the credit limit for a customer's credit card account. A failure to properly assess an application for a credit card may lead an account-holder to incur a debt that he/she cannot service and may amount to maladministration by the financial institution in the decision to lend. Disputes of this kind are dealt with in accordance with the Ombudsman's maladministration policy (see page 23).

It follows that if a financial institution provides credit to a level which is substantially above the approved credit limit, there is also a risk that the lending will:

- Not be in accordance with the financial institution's lending guidelines;
- Not be able to be serviced by the account-holder;
- Be unconscionable;
- Amount to maladministration in the decision to lend, with the result that the financial institution's right to recover the additional lending may be unenforceable.

Disputes received by BFSO

The disputes we have investigated of this kind include the following scenario:

> *The disputant had a credit card account with a limit of $3,000. She was unemployed. She was able to use her card to make purchases that led to a debit balance on the credit card account of more than $13,000. The financial institution became aware that the disputant had exceeded her credit limit when it was approximately 10% over the credit limit. It took some action to contact the disputant but did not manage the rising debt in accordance with its usual guidelines.*

BFSO investigation

In assessing whether there has been maladministration in the decision to lend by allowing a credit card limit to be exceeded, the Ombudsman will:

- Apply the criteria for maladministration in the decision to lend; and
- Investigate what actions the financial institution took to try to prevent the further provision of credit, where this was possible.

The questions we will ask include:

Q: Did the financial institution assess the account-holder's capacity to service the debt in accordance with its lending guidelines?

Q: Was the financial institution able to identify a clear repayment source for the debt created?

Q: Did the financial institution pay proper regard to the account-holder's other commitments and the loan amount and term?

Q: Did the financial institution follow its usual procedures in the management of the debt?

Q: What options for recovery of the card and stopping use of the card were available to the bank?

Q: When did these options become available?

Q: What steps did the financial institution take to contact the account-holder to discuss the use of the card over the credit limit?

Q: When were these steps taken?

Q: What steps did the financial institution take to capture the card?

Q: When were these steps taken?

Multiple Transactions Below Merchants' Floor Limits

Difficulties in assessing a dispute can arise when the credit card is used for numerous transactions below merchants' floor limits. This use can take the card over its limit. This practice is well known to financial institutions. The difficulty that arises is determining when such use takes the card limit so high that the provision of credit amounts to maladministration.

The approach this office takes is to look specifically at the procedures the financial institution has in place to monitor and deal with credit card use of this sort. We may ask:

Q: Over what period were the transactions processed?

Q: What procedures did the financial institution have to identify or monitor such a pattern of use?

Q: Did the financial institution follow its usual procedures?

Assessing loss

If maladministration is established, the next question, which has to be investigated, is what loss the account-holder has suffered and/or how the account-holder can be put back in the position he/she would have been in but for the maladministration.

The matters we will look at to determine loss include:

Q: Did the account-holder receive a benefit as a result of the disputed transaction?

Q: Are there items purchased by the account-holder which should be transferred to the financial institution so that the account-holder is put back in the position he/she would have been in but for the maladministration?

Credit Cards: Placing a Stop on an Account

Secondary Cardholders

It is common practice to require primary cardholders who wish to cancel a subsidiary card facility to return the subsidiary card.

Difficulties arise when there is a dispute existing between the primary and subsidiary cardholder that often means that the primary cardholder cannot obtain access to the subsidiary card.

The Code of Banking Practice requires banks to provide information to customers about how the subsidiary card can be stopped or cancelled. The code also indicates that a "stop" may not be effective until the subsidiary card is surrendered.

Therefore, those banks that provide limited stopping for their account-holders will set good banking practice.

A limited stop is the stop placed on the card to allow it to be captured at an ATM or when a merchant seeks authorisation for a transaction. The stop will not enable a bank to stop the card being used for purchases that are below a merchant's floor limit.

Cancelled Direct Debits

An issue, which has also arisen in the context of these cases, is whether a financial institution could take some sort of action on behalf of an account–holder when:

- An account-holder has disputed the transactions debited by a merchant;
- The credit limit of the card has been exceeded; and
- That merchant is continuing to debit the account periodically.

This office understands that it may not be technically possible for a financial institution to "stop" a merchant processing a direct debit to the account, however, given that the debit has been cancelled by the account-holder, the financial institution is obliged contractually to accept this cancellation (see pages 48 - 50). Therefore, in this situation, this office considers good industry practice requires that when a financial institution has been notified of this problem, the financial institution should ensure that all future transactions under the direct debit authority are charged back by the financial institution on behalf of the account-holder.

Credit Cards: Direct Debits

Another significant area of concern for disputants has been the account-holder's ability to stop direct debits being debited to his/her card account. This issue is particularly significant where the credit limit has been exceeded.

In this section, we set out our approach to the following issues:

1. The account-holder's contractual right to withdraw a direct debit authority;
2. Variation of the general rule by credit card conditions of use; and
3. The limited nature of that variation if the terms and/or placement of the clause in the conditions of use is inadequate.

General Right to Terminate a Direct Debit Authority

This office's view is that an account-holder is contractually entitled, as between itself and the financial institution, to:

1. Withdraw any authority given to a third party by notice to the financial institution; or
2. Instruct his/her financial institution not to accept a particular debit request.

Therefore, in the absence of specific provisions in the credit card contract, an account-holder is not compelled to revoke the previously provided authority directly with the third party.

Credit Card Contract

Many financial institutions' credit card conditions of use do provide for the cancellation of direct debit authorities.

Financial institutions' conditions of use generally stipulate that an account-holder must cancel a direct debit authority directly with the third party. That contractual requirement may be found in the conditions of use under:

1. The general or "Using Your Card" section; or

2. The "Cancellation of Card/Closure of Account" section; or

3. Both of the above sections.

A term in the general or "Using Your Card" section of the conditions of use requiring an account-holder to cancel the direct debit authority with the third party may be enforceable.

If such a term is limited by its words or by its placement to the "Cancellation of Card/Closure of Account" section and the account to which debits continue to be processed is not being closed or the card cancelled, then the term is unlikely to be enforceable.

Cancellation of Card/Closure of Account Section

This office's view is that usually provisions found in the "Cancellation of Card/Closure of Account" section of conditions of use apply only to situations in which a card is being cancelled or an account closed.

The limitation by words or the placement in the "Cancellation of Card/Closure of Account" section of the conditions of use, of an instruction to cancel an authority directly with the third party:

- Will usually be an inadequate warning to the account-holder that all direct debits must be cancelled in this way because the account-holder may not be cancelling or closing the account; and

- Will usually be unenforceable or not be able to be relied upon by the financial institution in a dispute about the acceptance of a direct debit to an open and ongoing credit card account.

Conclusion

In summary, this office's approach is that:

1. Where an account's conditions of use do not contemplate cancellation of direct debit authorities, an account-holder is entitled to instruct the financial institution to not accept direct debit requests from a particular third party;

2. Where an account's conditions of use include, in the "Cancellation of Card/Closure of Account" section, an instruction directing an account-holder to cancel an authority directly with a third party, and the card is not being cancelled or the account closed, usually the instruction would not apply to an account which was not being closed or cancelled and therefore may not be relied upon by the financial institution; and

3. Where an account's conditions of use include an unlimited instruction or an instruction in the general or "Using Your Card" section, an instruction directing an account-holder to cancel an authority directly with a third party, usually the financial institution could enforce or rely on such a clause in relevant circumstances.

BFSO investigation

Therefore the questions we will ask when investigating these disputes include:

Q: Did the account-holder instruct the financial institution, but not the third party, that direct debits from the third party to the credit card account should not be accepted by the financial institution?

If yes, the account-holder is entitled to do this and thereby stop the debit arrangement unless the conditions of use vary the general rule.

Q: Do the conditions of use for the card instruct account-holders that they must also cancel the direct debit with the third party?

Q: Is the instruction given only in relation to closing an account or cancelling a card?

If yes, then the account-holder usually would not be required to have also contacted the third party before the bank should stop the direct debit in the event that the account is being kept open and the card not cancelled.

Q: Is the instruction given in the general section of the conditions of use?

If yes, then the account-holder would need to cancel the direct debit authority with the third party as well as the financial institution in order to ensure the payment was not debited to the account.

Credit Cards - Merchant Enquiries

The Ombudsman has considered several cases where financial difficulties have been suffered by customers because of the financial services providers' practice of treating a merchant's request for confirmation that there are available funds in a credit card account as a request for authorisation for that amount.

Request for Confirmation of Available Funds Treated as Request for Authorisation

Because the financial services provider treats the enquiry as an authorisation request, once the request is approved, the available credit is reduced by the amount the subject of the enquiry. The *"authorisation"* will continue to have this effect on the cardholder's available credit for up to ten business days or until a transaction is actually processed to the account, whichever is sooner.

Effect on Customer

The effect is that a cardholder may find that he/she has no available credit even though his/her purchases and other charges to the account are well within the credit limit. Particularly where the customer is overseas at the time, the effect can be acute financial difficulty.

No Implied Contractual Right to Debit

The Ombudsman's view is that, unless a financial services provider has disclosed to customers the effect of these *"authorisations"*, there is no contractual basis for reducing the customer's credit limit. While there may be an agreement between the cardholder's financial services provider and the merchant's bank to treat these queries as authorisations, in most cases there is nothing in the agreement between the cardholder and the cardholder's financial services provider which:

- Authorises the financial services provider to treat these merchants' enquiries as requests for authorisation having an effect on the credit limit of the card;

- Puts the customer on notice of the effect of allowing an imprint or swipe to be taken of the card (which would give some basis for arguing that the customer has consented); or

- Allows the financial services provider to reduce the credit otherwise available to a customer in circumstances where the customer is not in default of the terms and Conditions of Use and has neither purchased goods or services nor expressly agreed to pay in advance by credit card.

Credit Cards – "Signature on File"

In travel related cases in particular, merchants present vouchers carrying the letters "SOF" (signature on file) in place of a signature. This may be done when there is a variation from the original price quoted for the travel for which a signed voucher has been obtained. A dispute then arises as to whether the increased cost was authorised by the cardholder.

The Ombudsman will look at whether:

- The sales voucher specifically authorises the travel agent to rely upon the signature given for one charge to later vary that charge and to make further charges;

- The sales voucher put the cardholder on notice that this may be done;

- The conditions of use included a definition of *"purchases"* which included a purchase made on the basis of a signature held on file;

- The conditions of use put a cardholder on notice that the financial services provider would accept the merchant's statement that it held a signature on file as the cardholder's authorisation for a charge; and

- The financial services provider had information to conclude that the purchases had been expressly authorised even though no voucher had been signed.

ELECTRONIC FUNDS TRANSFER ("EFT") INVESTIGATIONS

Brief History of the EFT Code

The history of the EFT Code in Australia dates back to September 1986, when a Commonwealth Government Working Group launched a document called "Recommended procedures to govern the relationship between the users and providers of Electronic Funds Transfer (EFT) Systems". That document was amended and relaunched in December 1989 as the Electronic Funds Transfer Code of Conduct ("EFT Code"). There were further amendments in 1991 and 1998, but during all this period the EFT Code was restricted to electronic transactions effected by card and PIN.

The Australian Securities and Investments Commission ("ASIC") convened a new working group to review the EFT Code during 1999. The objective of this review was to create a technology neutral Code which would cover all forms of consumer electronic funds transfers. ASIC published a revised EFT Code on 1 April 2001 and it took effect from 1 April 2002 for account institutions that have subscribed to it.

As well as covering card and PIN transactions, the revised EFT Code covers other forms of EFT transactions such as transactions initiated by telephone and internet (including credit card transactions made over the telephone or internet). Anticipating the development and introduction of new electronic facilities, the revised EFT Code also includes a section on consumer stored value products such as smart cards and digital cash. The main exclusions from coverage by the revised EFT Code are transactions authorised by manual signature (such as credit card purchases conducted in the presence of the merchant) and transfers to or from an account designed primarily for use by a business and established primarily for business purposes.

The text of the revised EFT Code is obtainable from the ASIC website: fido.asic.gov.au. ASIC also publishes a plain-english guide entitled: "Your guide to the EFT Code". The Banking and Financial Services Ombudsman ("BFSO") is the principal external dispute resolution body that investigates complaints about unauthorised electronic transactions by reference to the EFT Code. Apart from this policy and procedures manual, BFSO also publishes occasional commentaries on the EFT Code through its quarterly Bulletin. Comment on the revised EFT Code is contained in Bulletin No. 35 (September 2002) and Bulletin No. 37 (March 2003). BFSO Bulletins can be downloaded from the BFSO website: bfso.org.au.

Relationship between EFT Code and Terms and Conditions of Use

The main focus of the EFT Code is to set out the principles for allocating liability in disputes about unauthorised electronic funds transfer transactions.

Members of the public who hold accounts with an account institution may not necessarily be aware of the existence of the EFT Code. Their relationship with their account institution will be governed by the terms and conditions of use ("T&Cs") for each particular type of electronic banking facility. However, there should be no difference between an allocation of liability under the EFT Code and an allocation of liability under T&Cs. This is because clause 2.1 of the EFT Code provides that:

- account institutions will prepare clear and unambiguous T&Cs that reflect the requirements of the EFT Code;

- T&Cs are to include a warranty that the requirements of the EFT Code will be complied with; and

- T&Cs will not provide for or be effective to create liabilities and responsibilities of users that exceed those set out in the EFT Code.

All account institutions that are members of the BFSO scheme and that offer accounts with electronic access to their customers have notified ASIC that they have subscribed to the EFT Code and have warranted in their T&Cs that they will comply with the EFT Code. Therefore, the Ombudsman reaches decisions in relation to EFT disputes by applying the principles set out in the EFT Code.

Relationship in T&Cs between Liability Provisions and Security Guidelines

Account institutions usually include a section in their T&Cs dealing with the need for account holders to protect the security of devices (i.e. cards) and codes (i.e. PINs and passwords) that enable access to electronic banking facilities. Although previous versions of the EFT Code did not comment on the relationship between security guidelines and liability provisions in T&Cs, it was the Ombudsman's policy that liability could only be determined by reference to the liability provisions of the EFT Code rather than by reference to failure to observe security guidelines.

The revised EFT Code has clarified the matter by providing, in clause 5.8(b), that account institutions may:

- provide guidelines for users on ensuring the security of an access method that are consistent with the liability provisions of the EFT Code; but must

- clearly differentiate the guidelines from the circumstances in which an account holder is liable for losses resulting from unauthorised transactions; and

- include a statement that account holder's liability will be determined under the EFT Code rather than the security guidelines.

One consequence of the clarification provided by clause 5.2(b) is that an account institution would be in breach of the complaint investigation and resolution procedures were it to allocate liability for unauthorised transactions solely on the basis that a user had breached its security guidelines.

This is not to say that there is no point to security guidelines. They provide guidance to account holders about practical measures that can be taken to maximise the security of accounts and access methods. But, when unauthorised transactions do take place, the security guidelines cannot override the liability provisions.

EFT Code Provisions about Allocation of Liability

The EFT Code is very specific about the circumstances in which liability for unauthorised transactions may be allocated to an account holder. Liability may not be allocated for reasons other than those set out in the EFT Code. The liability provisions, set out in Clause 5 and its sub-clauses, can be summarised as:

- No liability in specified circumstances;

- Full liability in specified circumstances; and

- Liability limited to $150 in other circumstances.

No Liability

An account holder has no liability for:

- Losses caused by fraudulent or negligent conduct of employees or agents of account institutions, network partners or merchants;

- Losses relating to any component of an access method that is forged, faulty, expired or cancelled;

- (Where the access method uses a device), losses that occur before the user received the device or code, including a re-issued device or code;

- losses caused by the same transaction being incorrectly debited more than once to the same account;

- losses occurring after notification that a device has been misused, lost or stolen or that the security of codes has been breached; or

- losses resulting from unauthorised transactions where it is clear that the user had not contributed to such losses.

Full Liability

The account holder is liable for losses where:

- the account institution can prove on the balance of probabilities that the user contributed to the losses through fraud or contravention of certain specified requirements in the EFT Code; or

- the account institution can prove on the balance of probabilities that the user contributed to the 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 codes forming part of the access method has been breached.

Proof on the Balance of Probabilities

The requirement in the revised EFT Code for an account institution to be able to prove on the balance of probabilities that the user contributed to the losses indicates that the account institution must both:

1. Prove on the balance of probabilities that the user contributed to the losses in one of the ways specified in the EFT Code; and

2. Provide sufficient information to establish its case, to warrant BFSO calling on the disputant to respond.

In practical terms, this means that the onus of investigation is placed on the account institution. This is consistent with the requirement in clause 10.4(b) of the EFT Code that, when it receives a complaint about an unauthorised EFT transaction, the account institution is required to obtain from the user at least the information outlined in the Schedule to the Code. If the investigation is properly carried out, the account institution should have enough additional information, in conjunction with its own technical information, to make an appropriate allocation of liability.

BFSO's role is then to assess the information provided to it by both the bank and the disputant, subject to any required clarification, and decide whether we can establish on a balance of probabilities that the user contributed to the losses in one of the relevant ways.

BFSO's assessment of the available information will determine whether we support the account institution's allocation of liability, or whether we consider that there should be a different allocation of liability that results in compensation to the account holder.

Additional comment about "proof on the balance of probabilities" is contained in BFSO Bulletin No. 37, March 2003.

Contravention of Specified Requirements

For access methods that use a code or codes, a user contravenes the requirements of the EFT Code if they:

- voluntarily disclose the code(s) to anyone including a family member or friend; or
- where the access method uses a device, indicate the code(s) on the outside of the device or keep a record of the code(s), without making any reasonable attempt to protect the security of the code record(s), that is liable to loss or theft simultaneously with the device; or
- for access methods using code(s) without a device, keep a record of the code(s), without making any reasonable attempt to protect the security of the code record(s); or
- select a numeric code representing the user's birth date or an alphabetical code that is a recognisable part of the user's name; or
- act with extreme carelessness in failing to protect the security of all the codes.

Limited Liability

Provided that a code was required to perform the unauthorised transactions, and where the account institution cannot prove on the balance of probabilities that the user contributed to the losses, the account holder's liability is limited to no more than $150.

The limited liability clause, clause 5.5(c), makes three further statements about the application of limited liability:

- in determining whether an account institution has proved on the balance of probabilities that a user contributed to losses, all reasonable evidence must be considered, including all reasonable explanations for the transactions occurring;
- 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 probabilities that the user contributed to losses; and
- in determining whether a user had unreasonably delayed notification, the effect of any charges for notification or replacement of an access method must be taken into account.

Will Disputes about Limited Liability be Investigated?

BFSO sometimes receives disputes from account holders who consider that they should not be liable even for the limited amount of $150.

Provided that a code (i.e. a PIN or password) was required to perform the unauthorised transaction(s), BFSO considers that investigation into disputes about limited liability is not warranted, except where:

- the information provided to BFSO by the account holder; and
- the information provided in the account institution's response to the dispute;

indicates that the unauthorised transaction(s) should be considered under one of the "no liability" clauses.

Consequently, when an account institution limits an account holder's liability to $150, more often than not BFSO's response will be to advise the disputant that we cannot assist them any further.

Other Factors Effecting the Allocation of Liability

Losses that exceed transaction limit or account balance

Even where an account holder is otherwise fully liable, their liability does not include:

- losses that exceed the daily or periodic transaction limit for the access method, account or electronic equipment (or a combination of these);
- losses that exceed the balance of the account (including any prearranged credit limit); and
- losses incurred on any one account that the account institution and the account holder had not agreed could be accessed using the access method.

Exercising rights under credit card scheme rules

For unauthorised credit card transactions, account institutions shall not hold account holders liable for more than the liability there would be if the account institution exercised any rights it had under card scheme rules at the time the complaint was made.

Discretion to reduce liability

There is a discretion for an external dispute resolution body to reduce an account holder's liability where the account institution has not applied a reasonable daily or periodical transaction limit. "Reasonableness" is to be determined having regard to prevailing industry practice. The main test for exercising the discretion is whether the security of means used to verify that the transaction was authorised adequately protected the account holder in the absence of reasonable transaction limits.

Failure of institution system or equipment

In cases of system or equipment malfunction, account institutions will be responsible to users for losses caused by the failure of institution system or equipment to complete a transaction accepted by the system/equipment in accordance with the user's instructions.

Account institutions may not avoid obligations owed to 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.

No General Duty of Care

It is important to note that the EFT Code imposes no general duty of care on a user or account holder.

Innocent Party may have to Bear the Loss

In considering the implementation of these guidelines, it should be understood that at the individual transaction level it is rarely the account institution's fault that an account holder has suffered loss. Usually a third party has benefited from the transactions and the Ombudsman must determine who, as between two innocent parties, must bear the loss in accordance with the principles set out in the EFT Code.

There is a general presumption at law that an account holder should not be liable for unauthorised transactions on their account unless they contributed to those losses.

But when the means of authorisation is a PIN or password, rather than a signature, it is often difficult to determine issues of authorisation and contribution because there may be insufficient information to determine either the identity of the person who entered the PIN or password or the means by which knowledge of a PIN or password was gained.

The EFT Code deals with the problem of insufficient information by providing that an account institution may not allocate full liability unless it can prove on the balance of probabilities that the user contributed to losses. The difficulty that an account institution has in meeting this onus of proof means that many complaints about unauthorised transactions are settled by limiting the account holder's liability to $150.

A decision by the Ombudsman that an account holder's liability should be limited to $150 does not necessarily mean that the user did not, in fact, contribute to the losses. It only means that the account institution has not proved on the balance of probabilities that the user contributed, with the consequence that the account institution bears the greater part of the loss. Conversely, there are circumstances where an account holder may have to bear liability for $150, without necessarily having contravened the EFT Code in any way, because there is insufficient information to make it clear that the user did not contribute to the losses.

How does BFSO Approach an EFT Dispute?

Relevant Established Facts

The EFT Code requires a decision maker:

1. To make a decision based on "…all relevant established facts and not on the basis of inferences unsupported by evidence"; and

2. To consider "…all reasonable evidence…including all reasonable explanations for the transaction occurring".

Information Obtained from Account Institution

The starting place for any investigation is the Schedule to the EFT Code. The Schedule sets out the information to be obtained, where available and relevant, from a user who lodges a dispute concerning the authorisation of an EFT transaction. The Schedule reflects the requirements of Clause 10.4 of the EFT Code.

This office therefore requests account institutions to provide the following standard information in response to a dispute lodged with BFSO:

1. A copy of the information obtained from the user in accordance with clause 10.4 of the EFT Code and the schedule to that clause;

2. Copies of all documents relating to the financial service provider's investigation of the dispute, including:

   (a) an extract from the transaction log for the relevant EFT access method;
   (b) details of the last undisputed transaction;
   (c) details of the account holder/user's notification of the misuse, loss or theft of a device, or breach of code security; and
   (d) any other material relevant to the account institution's decision;

3. The nature and result of the account institution's inquiries as to whether or not there was any system malfunction at the time of the disputed transaction(s);

4. Details of any further transactions on the account occurring after the disputed transaction(s) but prior to the time the theft/loss of the card or breach of the security of the code(s) was reported;

5. Where the disputed transaction was conducted with card and PIN, whether and in what circumstances the card was recovered;

6. Relevant account and/or credit limits;

7. The daily transaction limit applying at the time of the disputed transaction(s) to the particular access method, account or electronic equipment;

8. Either the reference code identifying the Terms and Conditions applicable to the account at the date the disputed transactions occurred, or a copy of those Terms and Conditions;

9. Where the disputed transaction was conducted with card and PIN:

   (a) the date the card was issued;
   (b) the date the PIN was issued;
   (c) whether the PIN was system-generated or self-selected;

(d) if self-selected, the date of the last PIN change;

10. Where the disputed transaction was conducted by another access method, e.g. phone banking or internet banking:

    (a) a description of the method by which the user gains access to the access method, including mention of every identifier and code that must be input to gain access;
    (b) the date the account holder /user first requested access to the access method;
    (c) the date the account holder/user first selected the code(s)necessary to gain access to the access method;
    (d) the date of the last code change made by the account holder/user prior to the disputed transactions; and

11. Account statements covering the disputed transaction(s) and the three months prior.

As well as the standard information outlined above, BFSO routinely seeks additional information from account institutions according to the circumstances of each particular case.

Information Obtained from User

Depending on the extent to which the account institution obtained information from the user in accordance with the Schedule to the EFT Code, and depending on the information provided by the account holder when the disputed was lodged with BFSO, this office also routinely seeks additional clarifying information from the account holder/user. The type of information that might be sought includes:

1. Clarification about the transactions that are disputed;

2. For self-selected codes, the basis of selection;

3. For system-generated codes, whether a record was kept, where it was kept, whether the record was disguised and how it was disguised;

4. Circumstances in which the account holder became aware of the loss of a device or breach of code security, and how and when they notified the account institution; and

5. Any other relevant information that could account for the misuse of a card or the misuse of phone and internet banking facilities.

General Approach to Investigation

After collating all the information requested from the account institution and the account holder/user in a particular case, we assess the information according to the following criteria:

1. What are the relevant established facts?

2. Given the relevant established facts, what are all the possible reasonable explanations for the fact that the disputed transactions occurred. This will include an assessment of whether there is any possibility that the disputed transactions were carried out by the user or by some other person with the user's knowledge and consent, i.e. whether there is any possibility that the disputed transactions were authorised rather than unauthorised;

3. For each of the possible reasonable explanations about how the transactions occurred, what is the degree of likelihood that should be accorded to each of them;

4. What is the cumulative effect of this assessment about the likelihood of the relevant established facts in establishing that:

   (a) the user contributed to the losses; or
   (b) the user did not contribute to the losses;

5. Is the assessment sufficient to conclude that:

   (a) it is clear that the user did not contribute to the losses, such that the account holder has no liability; or
   (b) on the balance of probabilities, the user did contribute to the losses, such that the account holder has full liability; and

6. Should the account holder's liability be limited to $150, on the basis that the relevant established facts are not sufficient to prove on the balance of probabilities that the user contributed to the losses.

Allocation of Liability under EFT Code

The great majority of disputes considered by BFSO require the Ombudsman to form an opinion as to whether, on the balance of probabilities, the account institution has proved that the user contributed to the losses resulting from unauthorised transactions by contravening the requirements set out in clause 5.6 of the EFT Code (as summarised above), or by unreasonably delaying notification to the account institution.

We set out below our approach to assessment of the following concepts that govern the allocation of liability, namely:

- voluntary disclosure of codes;
- simultaneous loss or theft of device and code record;
- record of a code;
- self-selected codes;
- protecting the security of a code record;
- reasonable attempt to disguise a code;
- preventing unauthorised access to a code record;
- acting with extreme carelessness;
- unreasonably delaying notification; and
- credit card transactions on internet

Voluntary Disclosure of Codes

In assessing whether a user voluntarily disclosed one or more of the codes, the following principles apply:

1. There has to be an intention to disclose a code to another person. Ordinarily, mere entry of a code at an electronic terminal or equipment (including a computer or a telephone) is not "voluntary disclosure" when the intent of the user is to carry out an electronic transfer of funds;

2. The voluntary disclosure by the user must contribute to the losses for the account holder to be liable. This means that a causal connection must be established between the voluntary disclosure and the consequent losses. That causal connection might be lacking where, say, an account holder acknowledged having disclosed a code to a family member but the unauthorised transactions were carried out by an unrelated third party following theft of a card;

3. All other reasonable explanations, apart from voluntary disclosure, to account for how knowledge of a code became known must be assessed to determine which explanation is the most probable. For example:

    - was a user "shouldered" at an ATM or EFTPOS terminal by a thief?
    - did a thief find a code record that was reasonably disguised?
    - did a thief find a code record that was not disguised but was either stored separately from a card or stored in circumstances where reasonable steps had been taken to prevent unauthorised access to the code record?
    - did an internet banking password become known because a keystroke program was installed by an unauthorised third party on the user's computer?
    - did an internet banking password become known because the user mistakenly logged on to a fraudulent website that mimicked the appearance of the account institution's legitimate website?

The Ombudsman's view is that if a user discloses a code in the following circumstances, the disclosure is not made "voluntarily" for the purposes of clause 5.6 of the EFT Code:

1. The user is coerced into disclosure by force, duress, intimidation or threat;

2. The user gives in to persistent and sustained demands that amount to undue insistence or pressure;

3. The user is induced to disclose the code by a person in authority or a person that the user reasonably believed to be a person in authority (for instance, a police officer or a staff member of the account institution);

4. The user makes a reasonable mistake of fact or law that the code disclosure is authorised or required by the account institution or the law in the circumstances.

The assessment of whether or not a user should reasonably have believed that they were disclosing the PIN to a person in authority, or as a result of a mistaken belief that they were authorised, or compelled by law, to do so, will be assessed in light of the educative activities undertaken by the user's account institution about code security. At the same time, BFSO recognises that attacks on the security and integrity of the electronic banking system are increasing in sophistication, as demonstrated by the creation of fraudulent internet banking websites to capture account identification and password information. Accordingly, BFSO will take into account the extent to which the reasonable user of electronic funds transfer facilities could be expected to understand the means by which the security and integrity of the system can be circumvented, and to appreciate the extent of electronic fraud.

Simultaneous Loss or Theft of Device and Code Record

The revised EFT Code defines a device as "a physical device used with electronic equipment to access an EFT account". Most commonly, a "device" is a card that is used in combination with a PIN or password to access an account.

Card issuers warn that the best way to keep a code, i.e. a PIN or password, secure is to memorise it. However, this is not always possible. In assessing whether a user has contributed to losses by keeping a record of a code that was liable to loss or theft simultaneously with the device, the following principles apply:

1. A user may keep a record of the code linked to their device;

2. The user must not indicate the code on the outside of the device;

3. Preferably, the user should make a reasonable attempt to protect the security of the code record;

4. If the code record is not reasonably protected, it must not be:

    a) carried with the device; or
    b) kept in such a way that it could be lost or stolen simultaneously with the device.

There are two aspects to the concept of making a reasonable attempt to protect the security of a code record, which includes either or both of:

- making any reasonable attempt to disguise the code within the record; or

- taking reasonable steps to prevent unauthorised access to the code record.

Definition of "simultaneous"

During the development of interpretative policies for the 1998 version of the EFT Code, the Ombudsman received a number of submissions to the effect that "simultaneous" should be interpreted as meaning "in the same event".

The submissions were to the effect that if a thief broke into a cardholder's home and stole a card and a record of the PIN during the same burglary then this would reflect the intent of the EFT Code to make a cardholder liable if they kept their card and PIN record in such a way that they could be taken together. There are various gradations in this analysis: for example, the burglary could take 3 hours or a few minutes; the card and PIN record could be in the same room or different rooms.

It proved difficult to reconcile the plain meaning of "simultaneously" and the principle that a cardholder may keep a record of the PIN with the scenarios suggested by these submissions. Consequently, after considering his own external and internal legal advice, the Ombudsman developed principles for assessing the concept of "simultaneous" loss or theft. The same principles are relevant to assessment of liability under the revised EFT Code for loss or theft of device and code record.

The Ombudsman's view is that "simultaneous" loss or theft would occur where the device and code record are:

- in the same receptacle that itself can be lost or stolen (for example, a wallet, handbag, briefcase or suitcase); or

- in the same location within the same room (for example, on the same desktop or tabletop, or in the same drawer or box) so that device and code record can be seen together and taken in the same instant.

In the case of theft from a vehicle, however, the Ombudsman's view is that "simultaneous" loss or theft would occur when both device and code record were in the vehicle, even if they were in different compartments of the vehicle, e.g. the device in a centre console and the code record in the glove box.

Rationale

The rational for the Ombudsman's policy is that he has reached this view based on:

- dictionary definitions of "simultaneously";

- judicial interpretations of "simultaneously";

- the context of the phrases in the EFT Code; and

- the fact that while the EFT Code is concerned to ensure that users are not grossly negligent, the recognition that a code record may be kept only implies an obligation on the user to exercise a reasonable standard of care to keep a device and a code record a reasonable distance apart.

With regard to theft from vehicles, the Ombudsman's rationale is that a vehicle is a particularly confined space that facilitates the easy removal of any objects contained in that space.

Record of a Code

The 1998 version of the EFT Code contained no reference to the fact that account institutions had introduced systems that enabled cardholders to self-select a PIN of their own choosing.

The obvious intent of the self-select facility was that it enabled a cardholder to choose a PIN that they would remember easily, thus making it less likely that the cardholder would create their own PIN record – either at the time of or after choosing the PIN.

The problem that the Ombudsman faced was whether it could be said that a cardholder had contributed to losses where they self-selected a PIN that was a number or word that could be found on other cards or documents usually carried by the cardholder in their wallet, but the number or word:

- was created and kept for a purposes other than as a memorial of the PIN (e.g. a date of birth on a driver's licence); and/or

- pre-dated the selection of the PIN.

The problem typically arose in the context that the cardholder had self-selected their PIN to be the same as, or based on, their date of birth and information about their date of birth was contained on their drivers licence.

The policy that the Ombudsman developed for the 1998 version of the EFT Code was that a record of information created for purposes other than the recording of a PIN and/or a record of information created before the generation or selection of a PIN would usually not be considered to be a "record of the PIN" because:

1. The creation and keeping of a "record of the PIN" required an intention to create and keep the recorded information as a memorial of the PIN; and/or

2. *A transaction/event must occur before a record of the transaction can be recorded. In other words, you cannot have a record before the event to be recorded.*

Accordingly the Ombudsman considered that, because it was kept as a memorial in relation to their holding of a licence to drive, any record of information on a drivers licence would not be a memorial of a PIN. This meant that information such as date of birth on a drivers licence would not be a record of a PIN for the purposes of determining liability under the EFT Code. So, when he considered disputes under the 1998 EFT Code, the Ombudsman considered that a cardholder who self-selected a PIN to be the same as their birth date was not necessarily liable for unauthorised transactions just because they kept their card in the same wallet as a drivers licence on which their birth date was recorded.

Because it also covers telephone banking and internet banking, the codes for which are usually required to be nominated by the user, the revised EFT Code does acknowledge the existence of self-selected codes. It also recognises the dangers that arise from selecting a code that can be found on other cards or documents by proscribing the self-selection of the user's date of birth or name as a code.

So the practical guidelines developed after 1998 to deal with information that appeared on a document such as a drivers licence will not always apply to disputes under the revised EFT Code. However, the Ombudsman will still apply the same general principles when considering what constitutes a record of a code, namely that:

1. The creation and keeping a record of a code requires an intention to create and keep the recorded information as a memorial of the code; and

2. A transaction/event must occur before a record of the transaction can be recorded. In other words, you cannot have the record before the event to be recorded.

Self-selected Codes

A "code" is defined in the revised EFT Code to mean information:

- the content of which is known to the user and is intended to be known only to the user or only to the user and the account institution;

- which the account institution requires the user to keep secret; and

- which the user must provide (in any manner) to or through a device or electronic equipment in order to access an EFT account.

The definition of "code" thus encompasses both:

- PINs for cards (which are known only by the card user and which are not held on file by the account institution even though they may be generated by the account institution); and

- passwords for telephone banking and internet banking facilities (which are typically nominated by the user to the account institution and may be held on file by the account institution).

The revised EFT Code recognises that the security of self-selected codes can be compromised if the chosen code is so closely connected with the user that it could be guessed or ascertained from other information by an unauthorised third party. To counter the most obvious problems, without unduly limiting a user's ability to choose easily remembered codes, the revised EFT Code provides that a user contravenes the requirements of the EFT Code if they select a numeric or alphabetical code that:

- represents the user's birth date; or

- is a recognisable part of the user's name.

The proscription of these two types of self-selected code is not absolute. It applies only where:

- the code is chosen after the account institution subscribed to the revised EFT Code [generally, this date is 1 April 2002 - the date from which the EFT Code became binding on Code subscribers]; and

- immediately before selection, the account institution specifically instructed the user not to select either type of code and warned the user of the consequences of such a selection.

The EFT Code goes on to provide that, where this particular clause applies, the onus will be on the account institution to prove on the balance of probabilities that it gave the specific instruction and warning to the user at the time specified and in a manner designed to focus the user's attention specifically on the instruction and the consequences of breaching it.

Policies that will be followed by BFSO in the context of disputes about unauthorised transactions include that:

1. The EFT Code only restricts self-selected codes in the two specific instances. Otherwise, there are no restrictions on the type of code that can be selected;

2. Choice of the name or birth date of another person, such as a spouse/partner, parent or child, does not contravene the EFT Code;

3. The specific restrictions only apply to codes selected or changed after 1 April 2002. They do not apply to codes selected before that date;

4. Where a user disputes that, immediately before selection, they were given the instruction and warning BFSO will require the account institution to prove that it gave the instruction and warning. Such proof might be in the form of a signed acknowledgment by the user that they received the instruction and warning. In the absence of proof, BFSO would not automatically assume that the instruction and warning was given;

5. A provisions about self-selection of codes in T&Cs would not in itself be a *specific instruction* given *immediately before selection*; and

6. The wording of the revised EFT Code implies that, where the selection or change of code is done in the presence of a staff member of the account institution, the instruction and warning would normally be given orally. Where the selection or change of code can be effected through an ATM, computer, telephone or other electronic terminal or equipment, system software should insert a prominent instruction and warning at the relevant point of the self-selection program.

Protecting the Security of a Code Record

As mentioned above, protecting the security of a code record includes both of either making a reasonable attempt to disguise the code within the record, or taking reasonable steps to prevent unauthorised access to the code record. Both of these factors are considered separately below.

The concept of making a reasonable attempt to protect the security of a code record applies to both code records that are used in conjunction with a device, and to stand alone code records used in access methods such as telephone banking and internet banking.

A user is not required to protect the security of identifiers, that is: non-secret information such as account numbers, customer identification numbers, card number and card expiry date.

Where a code is used in conjunction with a device, the necessity to make a reasonable attempt to protect the security of the code record only applies where the code record is carried with the device or liable to loss or theft simultaneously with the device.

More care must be taken with codes used to access telephone banking and internet banking. For facilities that need only one code to gain access, a user may be liable for unauthorised transactions if any record of that code is found by an unauthorised person unless the user has made a reasonable attempt to protect the security of that code record. For facilities that need two or more codes to gain access, whether or not the user is liable will depend on whether the user kept the multiple code records on the one article, or on several articles liable to loss or theft simultaneously; and whether or not the user made a reasonable attempt to protect the security of those code records.

Reasonable Attempt to Disguise a Code

The Ombudsman's guidelines developed for the 1998 EFT Code are still relevant to the revised EFT code.

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

1. Concealing the number or word's identity as a code within the record by altering the content of the code. For example, by:

    - re-arranging the numerals or letters; or
    - substituting other numerals, letters or symbols.

2. Concealing the number or word's identity as a code within the record, without altering the numerals or letters in the code or their order. For example, by:

    - making it appear as another type of number or word; or
    - surrounding the code with other numerals, letters or symbols;

3. Concealing the code record's identity as a code record by placing the record in a location or context where it would not be expected to find a code. For example, by concealing the code on a piece of paper in a cookery book; or

4. Concealing the code using some combination of these different approaches.

Assessing reasonableness of attempt to disguise a code

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

Standard of attempt

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

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

The reasonable user

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

   The reasonable user is a person:

   - of average intelligence;
   - who does not have the knowledge and experience of a thief or account institution claims officer about the strengths and weaknesses of different types of disguises;
   - who has sufficient, but not specialised, computer skills when it comes to using facilities such as internet banking; and
   - who is aware of widely publicised warnings by their account institution and the Ombudsman about unsafe methods to disguise a code, and would not use such methods unless additional features of disguise were also used in an attempt to reasonably disguise a code.

Each case to be assessed individually

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

   - the speed with which the account was accessed;
   - the manner of disguise of the code;
   - the speed with which the account was accessed;
   - whether the correct code was used at first attempt; and
   - any other information surrounding the code in the record and the location and context of the record containing the code; and

Relevance of account institution's educative activities

5. In determining whether an attempt to disguise was reasonable or not, the Ombudsman will take into account any directions by the account institution about unreasonable forms of disguise that it has widely publicised to users and account holders or which appear in its T&Cs.

Educative activities

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

1. T&Cs;

2. Communications to the account holder and user, for example in letters, emails, and notations on account statements and mail-out material;

3. Educational material displayed in account institution 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 code are often penetrated by thieves and it is strongly suggested that users do not record their codes by:

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

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

3. Recording the code 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 code as a:

   - birth date;
   - postcode; or
   - telephone number;

   without additional features of disguise.

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

Preventing Unauthorised Access to a Code Record

The revised EFT Code allows that a user might not have contravened the requirements of the EFT Code by keeping a code record that was liable to loss or theft simultaneously with a device, if they took reasonable steps to prevent unauthorised access to the code record.

End Note 20 to the EFT Code then comments 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, by keeping a record of the code in a securely locked container or preventing unauthorised access to an electronically stored record of the code."*

Although the End Notes do not form part of the EFT Code, clause 20.3 provides that they may be used to interpret the EFT Code. Accordingly, the Ombudsman adopts the End Note as part of these guidelines.

In implementing this provision, the Ombudsman will consider disputes on a case by case basis. In general terms he will apply the following principles:

Hiding the code record among other records or in an unexpected place

This concept is similar to the Ombudsman's view that a code may be disguised by concealing the code's identity as a code record by placing the record in a location or context where it might not be expected to find a PIN; for example, on a piece of paper in a cookery book.

Where disputes occur in the context that an undisguised code record was liable to loss or theft simultaneously with a device, the type of situation that is likely to arise is where the undisguised code record is hidden among other entries in an address book, diary, personal organiser or such like that was carried along with a device in a handbag, briefcase, backpack or similar container.

Generally speaking the Ombudsman would not accept that such a record was in a place where a code record would not be expected to be found. However, according to the circumstances of a particular case, he would consider whether the undisguised code record was reasonably "hidden" among the other records.

With regard to codes for telephone banking and internet banking, an undisguised code hidden in a folder with other banking records could <u>not</u> be accepted as being in an "unexpected place". But such a telephone/internet code hidden in a folder unrelated to banking topics in a filing cabinet could be accepted as being in an unexpected place and/or hidden among other records.

Keeping the code record in a securely locked container

What constitutes a "securely locked container" would be assessed in the circumstances of a particular case. In general terms, the Ombudsman's view is that:

1. He would not be likely to accept that an undisguised code record was in a securely locked container where the code record and device were in:

    - a motor vehicle that was locked;
    - a brief case that was locked; or
    - a house that was locked.

2. He would be likely to accept that an undisguised code record was in a securely locked container if it was locked in a safe of robust construction and tamper-proof, keyless access;

3. Before accepting that storage in other lockable containers, such as filing cabinets, cupboards and lightweight home safes, constituted a "securely locked container", he would make an assessment of such factors as:

    - the robustness of construction;
    - the ease with which entry could be forced;
    - the probability that the container was routinely locked; and
    - the usual location of the key that controlled access.

Preventing unauthorised access to an electronically stored record

An electronically stored record could be stored in a program on a personal computer, lap-top computer, hand-held electronic organiser, mobile phone or such like electronic equipment.

In considering whether a user had taken reasonable steps to prevent unauthorised access to a code record stored on such electronic equipment, the Ombudsman would take into account factors such as:

- was information on the electronic equipment freely available through mere possession of or access to the equipment?
- was access to the electronic equipment restricted by the need to enter a password to gain access?
- was password access routinely turned on?
- was information stored under immediately recognisable menu items such as "bank passwords" or "account access codes".

Acting with Extreme Carelessness

The concept of contributing to losses by acting with extreme carelessness in failing to protect the security of all the codes was introduced with the revised EFT Code.

In assessing whether a user should be liable on the grounds of extreme carelessness, the Ombudsman will be guided by the comments in End Note 17 to the EFT Code. Accordingly, the Ombudsman's view is that:

1. "Extreme carelessness" means a degree of carelessness with the security of the codes that greatly exceeds what would normally be considered careless behaviour;

2. The concept of extreme carelessness does not apply to the selection of codes, which is treated separately in the EFT code by the proscription of codes linked to the user's birth date and name; and

3. The concept of extreme carelessness does not apply to the security of identifiers, which are not required to be kept secret.

End Note 17 gives as an example of "extreme carelessness" a situation where a user stored their user name and password for internet banking in a diary or personal organiser or computer (not locked with a PIN) under the heading "internet banking codes".

Unreasonably Delaying Notification

A user contributes to losses resulting from unauthorised transactions if they unreasonably delay notification to their account institution after becoming aware of the misuse, loss or theft of a device, or that the security of code(s) has been breached.

The revised EFT Code, in sub-clause 5.5(b), goes on to provide that 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.

The revised EFT Code also comments, in sub-clause 5.5(c), 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.

The Ombudsman takes the following view when assessing the two times from which delay in notification could be measured:

Actual awareness

As a first step the Ombudsman will make an assessment of the time at which the user actually became aware of the misuse, loss or theft of a device, or that the security of code(s) had been breached (e.g. by becoming known to an unauthorised third party).

For a user to actually become aware of this fact requires more than doubt or suspicion. For example:

- usually, a user will need to check that a device has not been misplaced before they actually become aware that the device has been lost or stolen;

- usually, a user's doubts or suspicions that someone may have seen them enter a code at a terminal will not make them actually become aware that the code has become known to someone else; and

- for a user to become aware that the security of an access code for telephone or internet banking has been breached, it would usually be necessary for them to actually become aware that unauthorised transactions appear on the account or, at least, that the account balance is significantly less than expected. However, the mere fact that account statements were sent to the account holder would not in itself mean that the account holder actually became aware of unauthorised transactions at the time the statement was sent.

Should reasonably have been aware

In the case of loss or theft of a device, an account holder's liability commences from the time that the user should reasonably have become aware of the loss or theft. Note that this test does not apply where a device has only been misused (i.e. not lost or stolen) or when code security has been breached.

The time at which a user "should reasonably have become aware" arises when a reasonable user, with the actual user's pattern of card use and in the actual user's circumstances at the time, would reasonably have checked on the presence of the device, either to use it or to confirm that the card was still in their possession, in such circumstances as:

- where there is evidence of theft or attempted theft, which would make a reasonable person check the presence of their card . (For example, where there has been a burglary, the user's home or office has been rifled, or there has been an attempt at pick-pocketing); or

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

The test of when a user should have checked the whereabouts of their device does not impose an obligation on the user to regularly use the device. The test is subjective. This means that the Ombudsman would look at the user's usual practices and their explanations for any variation from that practice.

It is not an unreasonable delay for the user to take a reasonable time to ensure that 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 account institution. Nor, if they become aware of the loss or theft within branch opening hours, is it unreasonable delay for the user to notify a branch rather than use the account institution's telephone hotline or customer contact line. Furthermore, delays in notification caused by congestion on a telephone line or in a branch are not unreasonable delays by the user or account holder.

Delays because of doubt or suspicion and/or because of the effect of charges

The requirement to take into account the effect on the user of charges is illustrated by the following scenario:

- there was unauthorised access to an account using a card and correct code;
- the account institution denied the claim on the basis that the user unreasonably delayed notification; and
- the user delayed contacting the account institution because they were unsure whether they had lost the card and did not want to unnecessarily incur the inconvenience and costs associated with obtaining a replacement card.

If a user takes this option then the user is:

- allowing a thief more time in which to access the account; and
- putting themself in a position where they may have to show that they 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 user had good grounds for doubting that the card had really been lost or stolen;
2. Whether the user had previously incurred this inconvenience and cost unnecessarily;
3. Whether the user's finances were so delicately placed that their decision would be affected in this way; and
4. How much longer the search took as a result of this concern about those costs, e.g. 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:

1. before the user actually became aware or should reasonably have become aware of the loss of theft of a device; or
2. while the user is reasonably:
    - ensuring that the card has not been misplaced; or
    - searching for the card; or
    - notifying police or security officers;

- before notifying the account institution or making a reasonable attempt to notify the account institution;

then the user does not contribute to the loss from that unauthorised transaction and the account holder would not be liable on the basis that the user unreasonably delayed notification.

Credit card transactions on internet

Liability for unauthorised credit card transactions effected by quoting a card number and expiry date over the internet has been subject to the liability provisions of the EFT Code since 1 April 2002. Some of the consequences that follow from this extension of EFT Code coverage are:

1. An account institution may not seek to restrict or deny account holders their rights to make claims or to attempt to impose time limits on users to detect errors or unauthorised transactions [clause 4.4]; and

2. 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 [clause 2.1].

Relationship between chargeback rights and allocation of liability

Unauthorised internet card transactions that are reported to the card issuer within chargeback time frames are usually resolved to the satisfaction of the account holder because the card issuer has been able to exercise its charge back rights.

The disputes that are brought to BFSO generally involve circumstances where the account institution's charge back rights have expired by the time unauthorised internet-based credit card transactions were brought to it's attention. However, because these transactions are covered by the EFT Code, the issue of account holder liability has to be considered as an entirely separate issue to whether or not the account institution still retains chargeback rights.

Even where the card-issuing institution is unable to charge back to the merchant institution, liability may only be allocated to the account holder according to the standard liability provisions of the EFT Code.

Liability for transactions made without the use of a secret code

Because internet-based credit card transactions only require the input of non-secret identifiers (i.e. card number and expiry date), without the need to input a secret code, the EFT Code limits the circumstances in which an account holder could be liable for unauthorised internet-based transactions.

End Note 4 to the EFT Code comments, among other things, that:

- "The inclusion of non-secret "identifiers" means that the use of an account number or card number at electronic equipment, without a device or secret

code, now comes within the scope of the EFT Code (e.g. use of a credit card number through telephone or personal computer to make a purchase)"; and

- "The user is not liable for unauthorised transactions based on the use of an identifier without a code or a device. The user is liable for unauthorised transactions based on the use of a device (or a device and an identifier) without a code only where the user unreasonably delays in notifying loss or theft of the device."

The general conclusion to be drawn from End Note 4 is that an account holder has no liability for unauthorised internet-based credit card transactions. This conclusion is supported by a close examination of clause 5.5(b) of the EFT Code – the clause that deals with the allocation of liability because of unreasonable delay in notification.

Does unreasonable delay in notification apply to unauthorised internet transactions?

Clause 5.5(b) allows an account institution to allocate liability for unauthorised transactions to the account holder where it can prove on the balance of probabilities that the user contributed to losses by:

1. Unreasonably delaying notification after becoming aware of the misuse, loss or theft of a device forming part of the access method; or

2. Unreasonably delaying notification after becoming aware that the security of all the codes forming part of the access method has been breached.

Point 2 above is usually not applicable to internet-based disputes because the entry of a code did not form part of the access method.

Where unreasonable delay does apply, 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.

Where the device (i.e. the card) was not lost or stolen, neither the account institution nor the Ombudsman can propose a time from which the account holder should "reasonably have become aware". Rather, liability can only commence from the time of actual awareness of the misuse of the card. Even then, there could only be liability on the basis of unreasonable delay if a misused device formed part of the access method.

For internet-based credit card transactions, identifiers input into a computer are the primary access method. Whether or not the "unreasonable delay" clause is applicable turns on whether or not the device (i.e. the card) also formed part of the access method. However, it does not seem that the device forms part of the access method for internet-based transactions because:

1. "Device" is defined to mean a physical device used with electronic equipment to access an EFT account;

2. The access method for internet-based card transactions only requires the card number and expiry date to be keyed-in at a computer terminal;

3. There is no physical interaction between a device and the computer terminal. This distinguishes internet-based transactions from ATM and EFTPOS transactions where the device is inserted into or swiped through the terminal; and

4. Internet-based transactions can be performed by a person who has never physically possessed or even sighted a device because all that is required to perform a transaction is knowledge of the card number and expiry date.

Where a device does not form part of the access method, there can be no contribution to losses on the basis of unreasonable delay in notification. Therefore, as all other possible reasons for allocating liability are eliminated because the access method does not use a code, there does not seem to be any basis in the EFT Code by which liability can be allocated to an account holder for unauthorised internet-based credit card transactions.

Even if a device did form part of the access method, liability on the basis of unreasonable delay in notification could only commence from the time that the account holder actually became aware of the misuse of a card. However, even though they may concede that they received statements, opened them and read the account balance, it could still be the case that an account holder who does not check each transaction in detail could still be unaware of unauthorised transactions.

In internet card disputes, the Ombudsman cannot determine that an account holder should reasonably have become aware of unauthorised transactions at the time of opening statements, because the "should reasonably have become aware" test can only be applied where a card has been lost or stolen. The "should reasonably have become aware" test cannot be applied in circumstances where the account holder still has a card in their possession, and the transactions result from misuse of the card number.

Failure to Properly Investigate a Dispute

Complaint investigation procedures

When a user disputes a transaction with their account institution, the EFT Code sets out a number of procedures for the allocation of liability and the investigation and resolution of disputes. In summary, the account institution is required to:

1. Obtain from the user at least the information outlined in the Schedule to the EFT Code;

2. Consider all reasonable evidence, including all reasonable explanations for the transaction occurring;

3. Make its decision on the basis of all relevant established facts and not on the basis of inferences unsupported by evidence;

4. Allocate liability, as between the account holder and the account institution, according to the circumstances in which the account holder is liable in full or in part, or when the account holder is not liable;

5. Complete its investigation within 21 days or receiving relevant details of a complaint or advise the user in writing of the need for more time;

6. Where it has advised the need for more time, complete its investigation within 45 days unless there are exceptional circumstances;

7. Where an investigation continues beyond 45 days, provide monthly updates to the user; and

8. Advise the user in writing about the outcome of the investigation, together with reasons for the outcome including references to relevant clauses of the EFT Code and, except where the complaint is resolved completely in favour of the user, contact details for its external dispute resolution body.

While the time frames mentioned above are generally applicable, the revised EFT Code substitutes different times where the disputed transaction concerns a credit card account and the account institution decides to resolve the complaint by exercising its rights under the rules of the credit card scheme:

- the time limits under the rules of the card scheme apply in lieu of the 21 and 45 day limits; and

- where an investigation continues beyond 60 days, the account institution is required to provide updates to the user every two months.

Where an account institution fails to observe any of these procedures, and where the failure contributed to a decision against the account holder or delayed the resolution of the complaint, the external dispute resolution body may determine that the account institution is liable for part or all of the amount in dispute.

Relevant established facts

What is important is that the account institution obtains sufficient information, appropriate to the circumstances of the complaint, to enable it to carry out the investigation required by clause 10 of the revised EFT Code. This should mean that when the account institution comes to assess how liability should be allocated, it will be able to make that assessment on the basis of "*relevant established facts*" rather than on the basis of "*inferences unsupported by evidence*". In many cases of unauthorised access, it is very difficult to determine how a code (PIN or password) became known to the person making the unauthorised transaction. In such cases the account institution has to consider all reasonable explanations for the transaction occurring.

Full liability may not be allocated to the account holder unless the "*relevant established facts*" are sufficient to allow the account institution to prove on the balance of probabilities that the user contributed to the losses within the narrow confines of the

EFT Code. Where the "*relevant established facts*" are not sufficient to provide such proof, the account holder's liability must be limited to no more than $150.

Reliance on access with correct access method

If an account institution fails to investigate a complaint and simply allocates liability for a disputed transaction on the basis that the user must have either disclosed the code or kept a record of the code because the account was accessed with the correct access method, then the account institution may have failed to observe the complaint investigation procedures for a number of reasons including that:

1. "Access with correct access method" is not one of the specific circumstances by which a user is deemed to have contributed to losses;

2. The EFT Code provides that 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 probabilities that the user contributed to losses;

3. The account institution may not have collected from the user at least the information specified in the Schedule to the EFT Code;

4. The account institution may not have considered all reasonable evidence, including all reasonable explanations for the transaction occurring;

5. The account institution may not have given reasons for the outcome of its investigation that include references to relevant clauses of the EFT Code and/or may not have given contact details for its external dispute resolution body.

Therefore, if an account institution allocates liability for a disputed transaction solely because access to the account was made with the correct access method and it failed to carry out any further investigation into the circumstances of the complaint, it may become liable for part or all of the amount in dispute if BFSO determines that the account institution's failure contributed to its decision or delayed the resolution of the complaint.

Time for completion of an investigation by an account institution

The Ombudsman's view is that if an account institution takes more than 45 days to complete an investigation then this is, on the face of it, an unreasonable delay by the account institution and, therefore, a potential breach by the account institution of clause 10.12 of the revised EFT Code.

To avoid being in breach of EFT Code requirements, the account institution would have to be able to show that there were "*exceptional circumstances*" which caused the delay, and that it wrote to the user to advise them of the reasons for the delay. The only other circumstance in which the revised EFT Code allows an investigation to extend beyond 45 days is where the account institution is waiting for a response from the user and has advised the user that it requires such a response.

End Note 23 comments that "*exceptional circumstances*" may include delays caused by foreign account institutions or foreign merchants being involved in resolving the

complaint. The Ombudsman does not consider that systematic delays resulting from the level of resources allocated to dispute resolution would constitute "*exceptional circumstances*" for the purposes of the EFT Code.

Where the complaint involves a credit card transaction, and the account institution decides to exercise its rights under the card scheme rules, the Ombudsman will have regard to the time limits allowed by the card scheme rules.

Under the provisions of the revised EFT Code, any failure of the complaint investigation procedures that delays the resolution of a complaint allows the Ombudsman to exercise a discretion to determine that the account institution is liable for part or all of the amount in dispute.

The discretion can be exercised simply to compensate the account holder or user for the effects of the delay, even where the account holder is otherwise liable for the amount in dispute.

Before determining that an account institution had failed to observe the applicable procedures, and that its failure contributed to the account institution's decision or delayed the resolution of the complaint, the Ombudsman would usually:

1. Advise the account institution of the reasons for concluding that it had not handled the complaint in accordance with the EFT Code;

2. Indicate to the account institution the reasons why this failure contributed to the account institution's decision, or delayed the resolution of the complaint; and

3. Request the account institution to provide explanations for why it handled the complaint in the way it did, and why it took the time it did to resolve the complaint at the account institution level.

After considering the account institution's explanation the Ombudsman would determine, in the circumstances of the particular case, whether liability for part or all of the amount in dispute should be borne by the account institution.