FINANCIAL OMBUDSMAN SERVICE

BULLETIN NO 29 – JUNE 2001
Direct Debits

In March 2000 this office published our proposed approach on the new system of Direct Debits to transaction accounts - see Bulletin 24. We stated that we would review our approach within 12 months and revise it if necessary.

On review, our approach will remain unchanged and will apply to complaints received about direct debits to transaction accounts.

An important part of our approach concerns the cancellation of direct debits and claims about unauthorised debits. The problems which may be experienced by bank customers seeking to cancel direct debits as, for example, in the case of One Tel customers seeking to cancel their direct debit authorities on the insolvency of One Tel) or obtain a reversal of an unauthorised debit are such that it is worth again setting out our approach.

Our approach reflects the provisions of the Australian Payment Clearing Association's rules, the Bulk Electronic Clearing System (BECS) rules which specifically set out rights on the part of accountholders to cancel direct debits in writing with their bank and to claim compensation, including re-crediting of the funds, through their bank.

Cancellation of Direct Debits

The authority may be cancelled by written notice to the bank

To the extent that a direct debit request is authority to a bank to debit a customer's account at the request of a third party, that authority may be cancelled by the customer either by notice to the third party *and/or* by notice to the bank. The APCA rules expressly state that a bank may not refuse to accept a cancellation in writing from a customer and must notify the third party of that cancellation.

Failure to accept or act on written notice of cancellation may cause compensable loss to the customer. In particular, a bank will not be able to recover costs such as overdrawing fees charged to an account on acceptance of a further direct debit after the customer has provided notice to the bank and will be obliged to re-credit the funds debited.

Claims in relation to Unauthorised Debits

The bank is obliged to process claims in relation to unauthorised debits

The APCA rules provide for a relatively simple and fast dispute process. A claim form may be completed at the bank, the third party's sponsor financial institution is notified and the third party must provide proof of authority within 7 days.

A bank will be in breach of the rules and its obligations to its customer if it refuses to process a claim in respect of an unauthorised debit on behalf of its customer. Refusal to do so may cause further compensable loss including loss of interest while the debit remains to the account and stress and inconvenience.

Old Passbook Complaints

Following the release of Bulletin Item 25 in June 2000, this office has considered a number of complaints by account-holders who say that a bank is unable to locate information supporting the existence of passbook accounts which were opened some time ago.

Usually, the account-holder had misplaced the passbook for a number of years and then rediscovered it at a later stage and wished to know what had become of the funds recorded in the uncancelled passbook.

There have also been complaints received from relatives who have located the passbook records of deceased account-holders and who make a claim for the funds shown in the passbook on the estate's behalf.

The Banks' First Responses to Complaints

The information which banks have provided in response to this office's requests for information show that the majority of the records that are kept by member banks date back seven years from the date of the complaint. However, the information has also revealed other available records which banks have retained for longer than seven years.

It has been this office's experience that an early search of all the bank's available records, to the extent that they are relevant to the circumstances of a complaint, can result in complaints being resolved at an early stage.

The provision of the results of these searches and copies of any relevant supporting information to this office (for example, a lost passbook declaration or unclaimed monies reports), prior to an investigation being commenced, assists this office to complete an investigation and draw conclusions, on the weight of the available information, where a complaint is unresolved.

<u>Information Available in this Type of Case</u>

Due to the small amount of positive information available in these types of cases, where the last transaction was many years ago, the assessment of these complaints is difficult and has been heavily reliant on an assessment of negative information (that is, information showing that an account was not in existence at a particular date).

This office appreciates that banks are not obliged by law to retain records for more than seven years from the date of the transactions covered by the records. However, in the interests of resolving these complaints more quickly and efficiently, it would be useful for banks to retain a computer record of closed accounts indefinitely, for instance, in CD ROM form.

This type of information could result in a greater number of complaints being resolved as it may confirm that an account has been closed and provide a date of closure. Additionally, it will assist this office to draw more conclusive views about the closure of an account.

Information about the Unclaimed Monies Fund

It has become apparent in the process of investigating these complaints that many account-holders are not aware that:

- their accounts could become inactive, inoperative or dormant if a transaction is not conducted on the account for a certain period of time;

- banks are under an obligation to transfer funds in its accounts to the Department of Treasury's Unclaimed Monies Fund if a transaction is not performed for a period of seven years; and

- interest would not be paid on the credit balance in the account once the funds are transferred to the Unclaimed Monies Fund.

This office accepts that many banks have established a practice of sending out letters to customers once an account becomes dormant notifying them of the impending transfer of funds in their accounts to the Unclaimed Monies Fund. This procedure is regarded as good industry practice.

Account-holders may be put on notice of this requirement at an earlier stage, if a reference in the terms and conditions of accounts is made to the possibility of the transfer of the funds to the Unclaimed Monies Fund, if no transactions are conducted for a period of seven years.

This type of provision may also prevent an assumption being made by customers that the funds will remain in the accounts until they make a request to withdraw the funds many years later. In reliance on this misunderstanding of the operation of their account, some customers have decided to leave funds in their passbook accounts for many years without performing any other transactions (in some cases, up to 50 years), when another form of investment may have been more suitable.

There could also be reference in the terms and conditions to any bank policy in regard to, for example, closing dormant accounts earlier and transferring the funds to an internal unclaimed monies account.

This Office's Procedure for the Consideration of Old Passbook Complaints

This office is currently in the process of simplifying and streamlining its complaints handling procedure for these types of complaints. The Ombudsman's Banking Adviser has requested further information from all member banks to assist in this process and to ensure that complete information is held by this office about the banks' records.

We anticipate that this review will result in these complaints being dealt with more efficiently in the near future.

The New Electronic Funds Transfer Code of Conduct

The new EFT Code was released by ASIC on 1 April 2001. It comes into effect on 1 April 2002 (unless a subscriber to the Code chooses to be bound by the Code at an earlier date). The following is a brief summary of some of the main points:

Coverage

The new EFT Code expands the coverage of the old Code. It comprises two main parts:
Part A covering electronic funds transfers and Part B covering consumer stored value facilities. There are also privacy and administration provisions in Part C and explanatory notes that do not form part of the Code but may be used to interpret the provisions of the Code. Part A, as well as covering card and PIN transactions, also covers other electronic funds transfers such as:

- Transfers between a customer's accounts by telephone and internet;
- Transfers to unrelated third party accounts by internet;
- BPay payments;
- Credit card transactions by phone or internet;
- Internet transactions paid with digital cash; and
- Transfers between an EFT account and a stored value facility.

The new EFT Code does <u>not</u> cover:

- Business funds transfers, i.e. that part of a funds transfer to or from an account that is designed primarily for use by a business and established primarily for business purposes;

- Any use of a stored value facility designed primarily for use by a business and acquired primarily for business purposes; and

- Credit card transactions that are authorised by signature.

Definitions

Because the new EFT Code covers wider types of transactions, it introduces new terminology and definitions. One of the more important new terms is *"access method",* which is the method whereby a user uses electronic equipment to access an EFT account. An access method comprises one or more components including devices, identifiers and codes or a combination of these. A *device* is a physical device used with electronic equipment to access an EFT account, such as a card. An *identifier* is information that the user is not required to keep secret, such as a card number and expiry date. A *code* is information known to the user, and perhaps to the bank, which the user is required to keep secret, such as a PIN or password. The distinction between an identifier and a code will be important when it comes to the allocation of liability for unauthorised transactions.

Terms and Conditions

As with the old Code, the new EFT Code requires account institutions to have Terms and Conditions that reflect the requirements of the Code. One new stipulation is that Terms and Conditions will not provide for or be effective to create liabilities and responsibilities of users, which exceed those set out in the Code.

Transaction Limits

Account institutions are required to inform a user about any restrictions on the use of an access method, including any daily transaction limit or other periodic limits that apply to the access method. The linking of transaction limits to the access method means that different types of facilities with different access methods can have different daily or periodic limits. For example, the daily limit for internet banking transactions could be different from the daily limit for card and PIN transactions. However, whatever limit is applied to the access method applies to all transactions with that access method. For example, all card and PIN transactions would be covered by an applicable daily limit, irrespective of whether they were performed at ATMs, EFTPOS terminals or branch teller terminals.

Allocation of Liability for Unauthorised Transactions

There are major changes in the new EFT Code to the way in which liability for unauthorised transactions is allocated. The liability provisions apply to transactions where the access method comprises one or more codes and/or a device. A user is not liable for unauthorised transactions where the access method comprises only an identifier.

Where a code was required to perform the unauthorised transactions, a user's basic liability is $150, unless it is clear that the user did not contribute to the losses (in which case the user would have no liability).

A user will be liable for the actual losses where the account institution can prove on the balance of probability that the user contributed to the losses through fraud or contravention of Code requirements. However, access with the correct access method will not of itself constitute proof on the balance of probability that the user contributed to the losses. A user may also be liable where the account institution can prove on the balance of probability that the user unreasonably delayed notification of either the loss of a device, or a breach of the security of all the codes. Liability for actual losses may not exceed any daily or periodic transaction limit, or the balance of an account (including any prearranged credit).

In summary, it is a contravention of Code requirements for a user:

- To voluntarily disclose one of more of the codes (i.e. the secret codes);
- To keep a record of one or more codes (without making any reasonable attempt to protect the security of the code records) that is liable to loss or theft simultaneously with a device;
- (Where the access method is one or more codes without a device), to keep a record of all the codes so that they are liable to loss or theft simultaneously;
- (After being instructed not to do so and been warned of the consequences), to self-select a numeric code representing the user's date of birth or an alphabetical code that is a recognisable part of the user's name;
- To act with extreme carelessness in failing to protect the security of all the codes.

How the Ombudsman will Consider Complaints

When considering complaints about the allocation of liability for unauthorised transactions under the new EFT Code, it is likely that the Ombudsman's approach will be to assess whether or not an account institution has proved on the balance of probability that a user contributed to the losses. This approach means that an account institution will need to ensure that there is full compliance with the complaint investigation and resolution procedures set out in the Code, at the time of its initial decision.

The Ombudsman will publish more detailed guidelines about the implementation of the new EFT Code closer to the date when the new Code comes into effect. In the meantime, any queries about the new Code can be directed to Laurie O'Keefe, by phone on (03) 9613 7326 or by e-mail to <LaurieOK@ABIO.org.au>