BULLETIN NO 37
Special Bulletin on EFT Investigations

MARCH 2003

In this Bulletin:

- Conducting investigations into EFT Code complaints – a practical guide
- The onus of proof in the EFT Code – its legal meaning and effect

Conducting Investigations into EFT Complaints

Our special Bulletin on electronic commerce in September 2001 included a detailed analysis of the requirements of the revised EFT Code in relation to investigation of disputes about unauthorised transactions.

In the following article, we approach the same topic from a different direction by discussing practical ways to ensure effective EFT investigations. The discussion is directed towards card and PIN transactions but the same principles are relevant to phone and internet banking transactions.

OMBUDSMAN

BULLETIN

The Australian
Banking Industry
Ombudsman Limited
GPO Box 3A
Melbourne 3001
Tel: (03) 9613 7373
or toll-free
1800 334 777
Fax: (03) 9613 7345

A.B.N. 48 050 070 034

Basic objective of an EFT investigation

The basic objective of an investigation into disputed transactions is to allocate liability in a way that is consistent with the EFT Code, bearing in mind that:

- Full liability can only be allocated to the account holder where the account institution can prove on the balance of probabilities that the user contributed to the losses; but
- 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 the losses; therefore
- The account institution should have additional information, apart from access with correct access method, that it relies on to support its decision; and
- The account institution must consider all reasonable evidence, including all reasonable explanations for the transaction occurring.

Collecting additional information

Account institutions routinely inspect transaction logs that record the disputed transactions. These logs only confirm that a user's card and the correct PIN for that card were used. The logs contain no information about how the card and knowledge of the PIN came to be in the possession of the person who made the disputed transactions. Therefore, the logs do not prove that the cardholder/user contributed to the losses.

The EFT code recognises the need to obtain additional information by specifying that account institutions must make reasonable efforts to obtain from the user at least the information outlined in the ***Schedule to Code***.

The type of additional information that should be considered in all investigations falls into two categories:

- Information known to or held by the account institution; and
- Information known to the user/account holder.

Information known to the account institution

Information known to or held by the account institution that should be taken into account includes:

- Transaction logs for disputed transactions, including both approved transactions and transactions denied for reasons such as incorrect PIN, invalid account, insufficient funds etc;
- Transaction log for last valid transaction;
- History of card used for disputed transactions, and prior cards under same number, including date of original issue, date replacement cards issued, expiry date, whether primary or secondary, time and date of cancellation etc;
- History of PIN, including date of original issue if system-generated and date of PIN change if self-

selected. [Best practice for account institutions is to maintain reports that log the time and date of PIN changes, or at least the latest PIN change].

- Account statements covering the disputed transactions and both prior and subsequent valid transactions; and

- User history, including all accounts held by user, all cards issued to user, details of how cards and accounts are linked, and whether user has access to phone banking and internet banking facilities.

Information known to user

Information that should be obtained from the user includes:

- Whether a device (card) was signed;

- Whether a code was self-selected and, if so, the basis on which the code was selected;

- If code was self-selected, whether or not the user was informed immediately before selection not to choose a code representing user's birth date or code that is a recognisable part of user's name;

- Date and time user became aware of loss of theft of device, or that security of code(s) breached;

- Date and time of report and means by which user reported to account institution;

- Date and time of report to police/other authority;

- If a record of a code was made (including retention of original PIN mailer), how it was recorded and where the record was kept;

- If a record of a code was lost, the date and time of that loss;

- Whether a code had been disclosed to any other person;

- How and where the loss of a device occurred (e.g. housebreaking, break-in to car, purse/wallet/bag stolen from home/shops/workplace etc); and

- Any other information about circumstances surrounding loss or theft of a device, or breach of code security, or reporting to account institution, or steps taken to ensure security of devices or codes that the user considers is relevant to the allocation of liability.

Obtaining this information requires the user to co-operate with the account institution. However, there is a practical motivation for the user to provide that co-operation because an account institution may delay resolving a complaint if it has requested information from the user and is waiting for a response.

Conducting the investigation

After collating internally available information and information collected from the user, the account institution is in a position to assess disputed transactions in the light of the available information and the EFT Code.

The standard required of an account institution is that it make a decision *"…on the basis of all relevant established facts and not on the basis of inferences*

unsupported by evidence." However, this does not preclude an account institution from drawing inferences that are based on facts apparent from the available information (e.g. if a cardholder had never used a card to make a PIN-authorised transaction, it is reasonable to infer that knowledge of the PIN was not gained from "shouldering").

Transactions authorised by the user

The liability provisions of the EFT Code do not apply *"…to any transaction carried out by the user or by anyone performing a transactions with the user's knowledge and consent."*

In a few complaints where, after careful assessment, the weight of information supports such a conclusion, an appropriate response may be that the transactions were made or authorised by the user and that the account holder is liable.

Great care should be exercised before reaching this conclusion because most complaints do involve unauthorised transactions. Note that access with correct access method does not, by itself, demonstrate that the user made the disputed transactions.

Assessing whether there is no liability

Where disputed transactions are accepted as unauthorised, the 1st step should be to assess whether or not the complaint falls into a category where there is **no liability** for the account holder. For example:

- Was the loss caused by the fraudulent conduct of an employee of a merchant, such as a supermarket checkout operator or taxi driver;
- Was the loss caused by a duplicated card created as a result of "skimming";
- Was the loss caused because a mailed-out card, or PIN, was intercepted before receipt by the user;
- Did the loss occur after notification that a card was lost or stolen; and/or
- Do the circumstances make it clear that the user did not contribute to losses?

Usually, there is not enough information to make it clear that a user did not contribute to losses. But, occasionally, sufficient information may be available; e.g. the person who made the unauthorised transactions is identified and they provide credible information about how they gained card and PIN, or were able to access passwords; or there is sufficient information to establish that a user was "scammed" at an ATM – with the card caught in a retractable sleeve and PIN entry captured by camera.

Assessing whether there is liability

If a dispute does not come under the 'no liability' clauses, the 2nd step should be to assess whether or not the user has contravened the requirements of the EFT Code or unreasonably delayed notifying loss of card/breach of code security.

The account institution has to be able to show that the contravention of EFT Code requirements contributed to the losses.

For example, sometimes a cardholder discloses a PIN to a family member. Where this is conceded in the context of unauthorised transactions, an account institution might allocate liability on the basis of voluntary disclosure. However, if the card was stolen by an unrelated thief and there is no linkage between disclosure to the family member and the thief gaining knowledge of the PIN, the cardholder has not contributed to the losses. In such circumstances, allocation of liability on the basis of voluntary disclosure is not appropriate.

An account institution needs to be continually assessing whether a PIN/password/code could have become known other than by contribution of the user, e.g. because of shouldering, or pinpad under camera surveillance, or record in separate location to card.

Voluntary disclosure of a code

Important principles to keep in mind include that:

- There has to be an intention to disclose the code to another person. Entry of PIN during the course of a transaction at an ATM or EFTPOS terminal is not ordinarily "voluntary disclosure" to people in the vicinity;

- There has to be a direct link between the disclosure and the unauthorised access;

- Disclosure, when it happens, may not always be voluntary, e.g:
  - where a user is coerced into disclosure by force, duress, intimidation or threat; or
  - where a user gives in to persistent and sustained demands which amount to undue insistence or pressure; or
  - where a user is induced to disclose the code by a person in authority or a person the user reasonably believed to be a person in authority (such as a police officer or bank officer); or
  - where a user makes a reasonable mistake of fact or law that code disclosure is authorised or required by the account institution or the law in the circumstances.

In assessing whether a user should reasonably have believed they were disclosing to a person in authority, or had a mistaken belief that they were compelled by law to disclose, the Banking Ombudsman would take into account the educative activities of the account institution about code security.

Simultaneous loss of device and code

Important principles to keep in mind include that:

- The EFT Code allows a user to keep a record of PIN;

- A user should not indicate a PIN on a card;

- A user should make a reasonable attempt to disguise a PIN record if they choose to keep a PIN record together with the card;

- Where a PIN record is not reasonably disguised it should not be carried with the card or kept in such a way that both card and PIN

could be lost or stolen simultaneously;

- Based on dictionary definitions and judicial interpretations of "simultaneously", the Banking Ombudsman's policy is that "simultaneous" loss or theft would occur where card and PIN are:
  - in the same receptacle which itself can be lost or stolen (e.g. wallet, briefcase, suitcase); or
  - in the same location within the same room (e.g. on same desktop or tabletop, or in same drawer or box) so that card and PIN record can be seen together and taken in the same instant; and

- In the case of theft from a vehicle, the Banking Ombudsman considers that "simultaneous" loss or theft would occur even if card and PIN record were in different compartments of the vehicle.

It would not be a case of simultaneous loss or theft where, during the course of a home burglary, a PIN record was found in a filing cabinet and a card was found elsewhere in the house

Reasonable attempt to disguise PIN/code

Important principles to keep in mind include that:

- Carrying a PIN record with a card does not mean that a user has contributed to losses where a reasonable attempt is made to disguise the code;

- The fact that a code disguise failed does not, of itself, make the attempt to disguise unreasonable;

- A reasonable attempt to disguise a code includes:
  - concealing the number's identity as a code by altering the content of the code, e.g. by re-arranging or substituting numerals; or
  - concealing the number's identity as a code within the record, without altering the numerals in the PIN or their order;

- The Banking Ombudsman will take into account any directions given by account institutions in Conditions of Use ("T&Cs") or mailouts to users; and

- The Banking Ombudsman's view is that some disguises are easily penetrated, and users should not use such disguises as:
  - birth dates, postcodes or telephone numbers without additional features of disguise; or
  - numbers marked or highlighted to indicate the code; or
  - numbers that stand out from surrounding information, e.g. 4 or 6 digit code among 8-digit telephone numbers.

Self-selected codes

Important principles to keep in mind include that:

- The EFT Code only restricts self-selected codes in two specific instances. Otherwise, there are no restrictions on the numeric or alphabetical codes that can be selected by users;

- The specific restrictions only apply to:

  - numeric codes which represent the user's birth date; and
  - alphabetical codes that are a recognisable part of the user's name.

  Choice of some other person's name or birth date would not contravene the EFT Code;

- In terms of allocation of liability, the specific restrictions only apply where:
  - The code was self-selected after 1 April 2002; and
  - Immediately before selection, the account institution specifically instructed the user not to select such a code and warned about the consequences of doing so; and

- A provision about self-selection in T&Cs would not in itself be a ***specific instruction*** given ***immediately before selection***. The EFT Code envisages something more designed to focus the user's attention, such as an oral instruction given before in-branch selection or a highlighted screen message for ATM/computer selection. The onus is on the account institution to prove that the instruction and warning were given.

Acting with extreme carelessness

The concept of acting with extreme carelessness in failing to protect the security of all the codes was introduced with the revised EFT Code. Important principles to keep in mind include that:

- ***Extreme carelessness*** does not apply to self-selection of codes;

- ***Extreme carelessness*** does not apply to identifiers, such as account numbers, card numbers and customer numbers;

- ***Extreme carelessness*** only applies to secret information, such as PINs or passwords needed for access to phone and internet banking;

- ***Extreme carelessness*** means a degree of carelessness with the security of the codes that greatly exceeds what would normally be considered careless behaviour (see endnote 17 of EFT Code). An example of extremely careless behaviour, given in end note 17, is storing the user's username and password for internet banking in a diary or personal organiser or computer (not locked with a PIN) under the heading "internet banking codes"; and

- Where access requires two codes, keeping an undisguised record of just one code would not constitute extreme carelessness.

Unreasonably delaying notification

Important principles to keep in mind include that:

- An account holder is not liable just because an unauthorised transaction occurred before notification that a card was stolen or that code security was breached;

- The issue to consider is whether the user contributed to the losses by unreasonably delaying notification after becoming aware of a lost card or breach of code security;

- In many cases, delay in notification will not contribute to an initial loss but could be a contributing factor to subsequent losses;

- Where something has happened to put a user on notice to check whether they still have possession of a card (e.g. home burglary or bag snatch), liability commences from the time the user should reasonably have become aware that their card was lost or stolen;

- It is not unreasonable delay for a user to take a reasonable time to search for a card, or to notify police or security before contacting the card-issuer; and

- Delay in notification caused by congestion on phone hot lines is not unreasonable delay.

Proof on the balance of probabilities

After considering all the available information, the final step is to consider whether or not the account institution can prove on the balance of probabilities that a user contributed to losses. Important principles to keep in mind include that:

- The onus of investigation is placed on the account institution. But significant information about unauthorised access lies with the user. However, as mentioned above, there is a practical motivation for users to co-operate in that the time for completing an investigation can be extended where information has been requested and the institution is waiting for a response;

- Proof on the balance of probabilities does not preclude the drawing of inferences on the basis of facts apparent from the available information. e.g. if a card has never been used with a PIN, it is reasonable to infer the user was not shouldered; and

- The mere fact that other possibilities exist does not preclude an allocation of liability based on the balance of probabilities. For example, at one extreme, every PIN entry is open to the possibility of shouldering. But the weighting to be given to the reality of this possibility depends on the circumstances of a particular case.

Final allocation of liability

After assessment of the relevant information in light of the EFT code, the final step is the actual allocation of liability. Important principles to keep in mind include that:

- If the account institution cannot prove on the balance of probabilities that the user contributed to losses, it should limit the account holder's liability to no more than $150;

- If the account institution is satisfied that it has proved on the balance of probabilities that the user contributed to the losses, it may allocate liability to the account holder for the full amount of unauthorised transactions except for:
  - Amounts that exceed daily or periodic limits; ;
  - Amounts that exceed the balance of the account or any pre-arranged credit limit; or
  - Amounts taken from an account which the institution and the account holder had not

agreed could be accessed by the access method; and

- Occasionally, an account holder may be liable for some but not all of the unauthorised transactions; e.g. a user might not have contributed to losses on the first day, but contributed to losses on the second and subsequent days because of unreasonable delay in notification.

Writing to the account holder

After an account institution has completed an investigation, it must inform the user about the outcome of the investigation;

Usually the advice will be in writing, except where the complaint is immediately settled to the satisfaction of both user and account institution;

As well as advising the outcome, the written advice must include:

- reasons for the outcome including references to relevant clauses of the EFT Code; and
- information about further action the user can take, including contact details for any external dispute resolution body;

Note that contact details for the external dispute resolution body must be given in the first letter advising the outcome of an investigation to a user/account holder. Unlike the old Code, the revised EFT Code does not allow for details of the external dispute resolution body to be withheld until senior management of an account institution has had a chance to review the first decision.

Effectively, senior management still get a chance to review because the external dispute resolution body refers all complaints back to the account institution. This change in the revised EFT Code is designed to speed up the final resolution of complaints.

Do's and Don'ts for investigations

Finally, here are a few tips for conducting an effective EFT investigation:

- **Do** collect all the information listed in the Schedule to the EFT Code;
- **Don't** automatically assume the account holder is liable because access occurred on first attempt;
- **Do** assess liability strictly according to the liability provisions of the EFT Code;
- **Don't** allocate liability on the basis that security guidelines in T&Cs must have been breached;
- **Do** take into account all reasonable explanations for the disputed transactions occurring;
- **Don't** allocate full liability unless the weight of information demonstrates that the user contributed by one of the specific means in the EFT Code;
- **Do** recognise that an account with electronic access is inherently less secure for an account holder than an account with signature access only. This reality underpins the EFT Code; and
- **Don't** attempt to allocate liability on the grounds that the account institution did not contribute to the unauthorised access and should not have to accept any of the losses.

The Burden of Proof in the revised EFT Code – its legal meaning and its effect on bank investigations and ABIO decisions

New provision as to burden of proof

The revised EFT Code requires the account institution to prove certain things on 'the balance of probability' [sic] in order for the account holder to be liable for losses. The effect of these words is that the EFT Code makes it clear that:

- the account institution has the burden (or onus) of proof and
- the standard of proof is proof on the balance of probabilities.

This is the first time that the EFT Code has contained a provision nominating one party as having a burden of proof. The provision has considerable legal significance. It does not necessarily require a change in the way the ABIO assesses information and reaches decisions. It does, however, require a shift in the way we will consider the information provided by the bank in response to the dispute because the provision makes it clear that the bank has the burden of proving contribution. This has legal meaning and effect. If the bank does not discharge this burden, we cannot find the account holder liable.

What is the burden of proof?

'The duty that lies on a party either to introduce evidence so that his case (or his particular defence) may be left to the jury [this is called the evidential burden] *or* to persuade the jury that he has established his case (or defence) [this is called the legal burden]. The *standard* of proof is the degree to which the party carrying a burden of proof must convince the court or jury that he has discharged it.' [Waight and Williams]

'The phrase "burden of proof has two senses…The first sense refers to the duty of a party to persuade the trier of fact by the end of the case of the truth of certain propositions…..This first burden is variously called the "legal burden", the "persuasive burden", the "burden of proof on the pleadings"…."the risk of non-persuasion"……

The second sense of "burden of proof" refers to one party's duty of producing sufficient evidence for a judge to call on the other party to answer,…The task of producing evidence fit to be considered by a jury is called the "evidential burden", the "burden of adducing evidence", or the duty "of passing the judge"…..

Failure to discharge the first burden [the legal burden] will cause the trier of fact to decide against the proponent on that issue; failure to discharge the second [evidential burden] will cause the judge to decide against the proponent without calling on his opponent or letting the case go to the trier of fact at all.' [Heydon]

Balance of Probabilities

The standard of proof in EFT Code cases is proof on the balance of probabilities.

The following is from Butterworths Encyclopaedic Australian Legal Dictionary

'**Evidence** The weighing up and comparison of the likelihood of the existence of competing facts or conclusions. A fact is proved to be true on the balance of probabilities if its existence is more probable than not, or if it is established by a preponderance of probability *(Rejfek v McElroy* (1965) 112 CLR 517; [1966] ALR 270; for example (CTH) Evidence Act 1995 s 140(1); (NSW) Evidence Act 1995 s 140(1)), or to the reasonable satisfaction of the tribunal of fact (*Briginshaw v Briginshaw* (1938) 60 CLR 336; [1938] ALR 334).

It is not a mechanical standard; it cannot be met by a mere mechanical comparison of possibilities independently of any belief in reality (*B v Medical Superintendent of Macquarie Hospital* (1987) 10 NSWLR 440) or of the nature and consequences of the fact or facts to be proved (*Briginshaw v Briginshaw*). Conversely, a statistical probability of less than 50 per cent does not necessarily mean that the balance of probabilities has not been met: *G v H* (1994) 181 CLR 387; 124 ALR 353.

Questions

It is not clear whether the drafters of the EFT Code intended the bank to have both the evidential burden of proof and the legal burden of proof. As a general proposition, however, the party bearing the legal burden generally bears the evidential burden. We have therefore assumed that the intention is that the bank will have the legal and evidential burden: it must prove on a balance of probabilities that the disputant has contributed to the loss in one of the relevant ways, that is, persuade us that we should find in favour of the bank in the case; and it must provide sufficient information to warrant calling on the disputant to respond.

Does this require a change in the way we collect information? Our current processes are to ask both parties for all relevant information in their possession. Does the change to the EFT Code mean that we have to ask the bank for all its evidence and then call on the disputant to answer it only if the scales are tipped against the disputant? What if the case is unclear on the information provided by the bank?

Comments

The new provision to do with onus of proof might be seen to be an unreasonable onus. After all, while the bank can produce technical information, such as whether the account was accessed with the correct PIN at first or subsequent attempts, this information proves only that the presumed thief has access to the PIN. It does not prove how the thief gained access and it does not of itself satisfy the bank's burden of proving that the disputant contributed to the loss in a relevant way. The important information on the latter issue is almost all in the possession of the disputant– did they keep a record and if so what and where was it kept, have they disclosed their PIN to anyone, if

there was a delay in reporting what was the explanation, if any.

The new provision needs to be seen, however, in the overall context of the Code. In practical terms it puts the onus of investigation onto the bank. This is consistent with clause 10.4(b) which provides that, where an account institution receives a complaint about an unauthorised EFT transaction, it is required to obtain from the user at least the information outlined in the Schedule to the Code. If the investigation is properly carried out, then the information provided by the bank to the ABIO should contain the relevant information about the user's habits and practices. In that sense the new provision underpins the investigation obligations and the stated consequences of not complying with them and ought not to be harsh in effect if the investigation is properly carried out.

As a comment, there is no mention of any obligation on the user to co-operate in the investigation. What should be the position of the bank if a user refuses to answer questions? As a practical matter our view is that there would be an implied obligation on a disputant to provide the essential information to the bank as a condition of having the dispute investigated further by the ABIO. Clause 10.6 is also relevant. It relieves the account institution from the obligation to complete an investigation within 45 days where the account institution is waiting on a response from the user. If, in a dispute that came to the ABIO, it was apparent that the disputant had failed to respond to the Schedule questions from the bank, our view is that it would be appropriate to discontinue the file until the investigation was able to be completed. In addition, our view is that the bank would not be expected to continue indefinitely an investigation if the disputant unreasonably failed to respond.

This is not an obligation on a disputant to answer all questions asked by the bank. It is an obligation to answer all reasonable questions asked by the bank in the course of its investigations to the best of the disputant's ability. In particular, it is not reasonably necessary in our view for a bank to require a disputant to report a suspected theft by a family member to the police as a condition of recovery under the EFT Code.

ABIO approach

The new provision does require a change in the way we assess the information we receive from the bank. It means that the bank, in response to a dispute, should produce to the ABIO all its information. We will then assess that information, subject to any required clarification, and decide whether it can establish, on a balance of probabilities, that the disputant contributed to the loss in one of the relevant ways. If the information does not establish a basis for liability to the requisite degree, we will not seek additional information from the disputant. Conversely, if it does then we will give the disputant the opportunity to respond and seek further necessary information from the parties in accordance with our procedures.

If we make the decision that the information provided by the bank is insufficient we will give the bank the opportunity to provide further information or submissions in relation to the information provided.

Assessing the possibilities

The law of evidence allows a court to make presumptions. Halsbury's Laws of Australia [195 2030] says that a presumption is an inference drawn, usually by logic or a statutory fiction, from one fact as to the existence of another. Presumptions are mechanisms for facilitating proof or directing a particular result. They may be of fact or law. Presumptions are at the heart of the view taken by courts that if certain facts are proved, then it follows that the defendant has been negligent (*res ipsa loquitur*).

Part of our decision-making process is to draw inferences on the basis of facts apparent from the available information. We assess the information and then include or exclude possibilities as to how the thief gained access to the PIN. Our decisions are usually made in the absence of the best evidence of how it occurred – a statement from the thief – and so inferences are a common ingredient in our EFT decisions.

Nothing in the new Code changes this. It is appropriate to continue, for example, to draw an inference that the disputant was not shouldered because of the established history of use of the card and PIN and the geographical or chronological information in relation to the unauthorised use. To the extent that we are engaged in assessing possibilities, the onus is on the bank to provide information that when assessed indicates that the explanation which is more probable than not is that the disputant contributed in a relevant way.

The obligation in relation to inferences, however, is only to draw them on relevant established facts.

When considering possibilities it is important to remember, as stated in *B v Medical Superintendent of Macquarie Hospital* (1987) 10 NSWLR 440, that the balance of probabilities is not a mechanical standard; it cannot be met by a mere mechanical comparison of possibilities independently of any belief in reality. 'The truth is, that when the law requires the proof of any fact, the tribunal must feel an actual persuasion of its occurrence or existence before can be found'. [Waight and Williams].

Fraud - the standard of proof

The application of the onus of proof on a particular head of contribution under the EFT Code needs to be mentioned. Clause 5.5 (a) provides for user liability where the account institution can prove on the balance of probabilities that the user contributed to the losses through the user's fraud or the user's contravention of the requirements of sub-clause 5.6.

The civil standard of proof of fraud is sometimes said to be higher than that for the proof of other issues – somewhere between proof on the balance of probabilities and proof beyond a reasonable doubt. This can be confusing. A good statement of what is required is 'that the nature of the issue necessarily affects the process by which reasonable satisfaction is attained….weight is to be given to the presumption of innocence and exactness of proof is expected' [Waight and Williams and see also *Briginshaw v Briginshaw* (1938) 60 CLR 336].

The ABIO will not reach or express a conclusion that a disputant has committed fraud - that is a decision which, because of its prejudicial nature, is more appropriately made by a court after all the evidence has been tested. But we can express a view that fraud has not been proved, if that is a basis on which the bank asserts that the disputant is liable. There may be cases where fraud is alleged but clearly not proven and it is helpful to the parties to reach a decision on the other issues in the case.

In addition, banks should not make this allegation lightly or without particulars of the allegation being provided. A mere assertion of fraud will be insufficient to raise it as an issue, whether for the purposes of a decision on the merits or for consideration of jurisdiction.

We welcome any comments or further discussion.