FINANCIAL OMBUDSMAN SERVICE

Banking & Finance - Bulletin 59
September 2008

In this issue:

Welcome to the first Bulletin from the Banking & Finance division of the Financial Ombudsman Service. We have, however, continued with the numbering system used by our predecessor, the Banking & Financial Services Ombudsman. So, in fact, this is Bulletin 59.

The Financial Ombudsman Service has been in operation for three months and the transition from the pre-merger schemes has gone smoothly. I would like to thank users of the Service for their support and co-operation during this transitional period. Our next big step will be the development and implementation of the new Terms of Reference by January 2010.

In the interim, it is business as usual as far as dealing with the disputes that come to the Service is concerned, and I trust that you find the following information about the introduction of PIN@POS useful. I would like to acknowledge the significant work done by our EFT Disputes Manager, Laurence O'Keefe, in putting this Bulletin together.

ISSN 1834-6510

Introduction

The Australian banking and card-issuing industry introduced the ability to authorise credit card purchase transactions by PIN at the point of sale on 4 June 2008. Known as "PIN@POS", the extension of PIN authorisation to cardholder-present merchant transactions offers benefits to cardholders, card issuers and merchants, but also changes the 'landscape' in which disputes about unauthorised transactions will be considered. The main change is that PIN@POS transactions come within the scope of the Electronic Funds Transfer Code of Conduct ("EFT Code").

This Bulletin is written from the perspective of the Banking & Finance division of the Financial Ombudsman Service in Australia. It deals mainly with the impact of PIN@POS on the resolution of credit card disputes, but includes comment on other EFT Code-related card issues.

Background

Holders of credit cards (such as MasterCard and Visa) in Australia have long been able to sign for credit card purchase transactions and to take cash advances from ATMs by inputting a PIN. They have also used their credit cards to make transactions over the phone or over the internet, just by entering the card number and expiry date.

PIN@POS introduces a new option by which a cardholder can authorise a purchase transaction at a merchant by entering their PIN into the EFTPOS terminal rather than by signing a paper voucher generated by the terminal.

For older-style cards issued in Australia, credit card data is encoded on a magnetic strip on the back of the card. Cardholders will be familiar with the type of EFTPOS terminal where the card is swiped through the terminal to allow the information encoded on the card's magnetic strip to be read by the terminal. However, magnetic strip cards have a degree of risk attached to them as it is possible to copy the information from a magnetic strip and make a cloned or 'skimmed' card. As part of an ongoing program to upgrade the security of credit cards, card issuers in Australia are rolling out cards that have a chip embedded in the card that contains all the information that identifies the card. Chip cards cannot be cloned or skimmed in the same way that magnetic strip cards can, so it is expected that chip cards will eventually lead to a reduction in credit card fraud.

However, chip cards require a different type of EFTPOS terminal because they are inserted into a slot in the terminal (rather than being swiped) and the card remains in the terminal until the transaction is completed. EFTPOS terminals that accept both chip and magnetic strip cards are being introduced progressively across Australia. However, it will be some time before all EFTPOS terminals are chip-enabled. Reflecting the gradual introduction of chip terminals, the chip-enabled cards that are being issued in Australia are, for the time being, hybrid cards that have the card data encoded on both a chip and a magnetic strip. Consequently, all cards can be used in all existing EFTPOS terminals. Over time, all terminals will be upgraded to accept chip cards and the final step in the process is likely to be the phasing out of magnetic strips on cards.

Unlike the situation in some overseas countries, where PIN-authorisation of credit card purchases is only available with chip-enabled cards, PIN@POS in Australia is available for cards with chips, cards with magnetic strips and hybrid cards with both a chip and a magnetic strip. The system in Australia is also marked by the fact that participation in PIN@POS is voluntary for the cardholder. When a credit card is swiped or inserted in a terminal and 'credit' selected as the account to be debited, the system will check that the card is a valid credit card and then give the cardholder a choice of either entering a PIN or pressing 'OK'. If the PIN is entered correctly, the transaction is authorised and a receipt is printed. If 'OK' is pressed, the terminal produces a voucher to be signed and the merchant is able to compare the signature on the voucher with the signature on the card before proceeding with the transaction.

EFT Code

The EFT Code is a voluntary industry code of practice covering all forms of consumer electronic payment transactions. The EFT Code is administered by the Australian Securities and Investments Commission ("ASIC").

Almost all credit card issuers in Australia subscribe to the EFT Code. By subscribing, they agree that they will comply with the requirements of the EFT Code and that their Terms and Conditions will not impose liabilities and responsibilities on users that exceed those set out in the EFT Code.

Financial Ombudsman Service is the main external dispute resolution service in Australia that interprets and applies the EFT Code to the resolution of disputes. Financial Ombudsman Service regards the provisions of the EFT Code as being the principal determinant of disputes about unauthorised consumer electronic payment transactions, because those provisions are effectively imported into the Terms and Conditions of any consumer facility offered by an account institution that subscribes to the EFT Code. Consequently, the provisions of the EFT Code take precedence if there is any variation between the liability provisions in the EFT Code and the liability provisions in the Terms and Conditions for a particular consumer facility.

In simple terms, the EFT Code covers all consumer transfers of funds that are made electronically, except that there is a specific provision that the EFT Code does not cover transactions that are authorised by manual signature. In terms of credit card usage, this has meant that cardholder-present transactions at a merchant, where the cardholder signs a voucher to authorise the transaction, have not been covered by the EFT Code even though the transaction itself is processed through electronic equipment. However many other credit card transactions do already come within the provisions of the EFT Code, including:

- Use of card and PIN to take cash advances from ATMs;
- Use of card without either PIN or signature to make transactions at terminals of a limited number of merchants such as car parks and service stations;
- Use of card by 'contactless' card technology to make low-value transactions at merchants such as fast food outlets and convenience stores;
- Use of a mobile phone as a 'virtual' credit card to initiate transactions that are debited to a credit card account;

- BPay transactions by phone or internet where payment is debited to a credit card account;
- Use of credit card number and expiry date over the phone or internet, to pay bills and purchase goods or services.

With the introduction of PIN@POS, cardholder-present merchant transactions also come within the scope of the EFT Code if the cardholder decides to authorise the transaction by PIN rather than signature. The expectation is that PIN@POS will reduce the incidence of credit card fraud, thereby producing benefits for cardholders, card-issuers and merchants. However the fact that such transactions will come within the provisions of the EFT Code has significant implications for both cardholders and card-issuers, which are discussed below.

The Impact of PIN@POS on Account Holders and Cardholders

Over time, the introduction of PIN@POS will produce benefits for account holders and cardholders. However, the fact that the new authorisation method is voluntary and, according to anecdotal information, not being taken up by cardholders as quickly as was projected means that all of the benefits will not come immediately. The benefits are expected to include:

1. A reduction in overall credit card fraud;

2. Quicker completion of PIN-authorised transactions, compared to the slight delay associated with the completion of signature-authorised vouchers; and

3. Disputes about unauthorised PIN@POS transactions will be resolved by reference to the EFT Code, including much longer time-frames in which disputes can be lodged because the EFT Code, as currently drafted, does not allow account institutions to impose time limits on account holders to detect errors or unauthorised transactions.

However, the introduction of PIN@POS also has the potential to increase an account holder's liability for unauthorised transactions, compared to the potential liability for signature-authorised transactions, if a cardholder does not take care to avoid contravening the requirements of clauses 5.5 and 5.6 of the EFT Code. In practice, this means that cardholders must always be careful to protect the security of their PIN, and always be careful to report the loss or misuse of their card without delay.

As discussed below, account institutions intend that PIN@POS transactions will have higher limits for cardholder-present-at-merchant purchase transactions than, say, the transaction limits that apply to PIN-authorised cash advances from ATMs. Consequently, an unauthorised person who obtains possession of a card and knowledge of the PIN for that card will be able to transact high amounts – up to the available credit – within a fairly short time if they utilise PIN@POS to make unauthorised transactions. In order to minimise their potential liability for unauthorised PIN@POS transactions, a cardholder must take care in the following areas:

Unreasonable delay in notification

The EFT code provides that the account holder is liable for unauthorised transactions where the cardholder unreasonably delays notification of the misuse, loss or theft of a card, or a breach of PIN security. In practice this means that a cardholder should report without unreasonable delay to the account institution that issued the card whenever the cardholder becomes aware that a card is not in their possession, or that someone else has used the card without permission, or that someone else has gained knowledge of the PIN.

Special care must be taken whenever a card is lost or stolen, because an account holder's liability commences from the time that the cardholder "*…should reasonably have become aware…*" of a lost or stolen card. Although replacing a card always involves some inconvenience for the cardholder, the risk of loss from unauthorised transactions means that it is always preferable to suffer minor inconvenience rather than suffer the losses that could arise from unreasonably delayed notification of a lost or stolen card.

Voluntary disclosure of PIN

The EFT Code provides that the account holder is liable for unauthorised transactions where the cardholder voluntarily discloses their PIN to anyone, including a family member or friend. With PIN@POS allowing for a greater number and a greater value of PIN-authorised transactions, the need for cardholders to be careful never to disclose their PIN is greater than ever.

Financial Ombudsman Service is aware that many members of the community disclose their PIN to a spouse, partner, other family members or a friend. This might be motivated by a culture of sharing within a family group or a desire for financial security in an emergency. But whatever the motivation, PIN sharing has the potential to render an account holder liable for unauthorised transactions. The experience of Financial Ombudsman Service in recent years is that a fair proportion of disputes about unauthorised transactions involve a family member or someone closely associated with the cardholder. So any disclosure by a cardholder may leave the account holder unprotected and liable for losses if it is the related party who uses their knowledge of the PIN to make unauthorised transactions.

Keeping a record of the PIN

The EFT Code provides that an account holder is liable for unauthorised transactions if the cardholder keeps an unprotected record of their PIN that is liable to loss or theft simultaneously with the card. Financial Ombudsman Service knows from our own experience that the number of people who make and keep a record of their PIN is reasonably high. The EFT Code allows that a PIN record may be kept. However, with the introduction of PIN@POS, it is possible that the consequences of keeping an unprotected PIN record with a card may affect a higher number of account holders for a greater amount in losses from unauthorised transactions. Consequently, it is in a cardholder's own interest to take great care to ensure that they keep the PIN record well apart from the card or, if they do keep the PIN record in close proximity to the card, to ensure that they either make a reasonable attempt to disguise the PIN or take reasonable steps to prevent unauthorised access to the PIN.

In the recent experience of Financial Ombudsman Service, many cardholders attempt to 'disguise' their PIN by writing it down as the last or first four digits of an 8-digit phone number. As the PIN is usually in its correct sequence, we do not usually consider that such a 'disguise' is reasonable. In some circumstances we might accept that the attempt to disguise was reasonable if the phone number was buried among a long list of names, addresses and phone numbers. But even here, a cardholder can negate their attempt to disguise if they list the disguised PIN under a name that draws attention to the likelihood of a PIN record being present. As an example, we have seen a recent dispute about a card branded with the name of a prominent retailer where the 'disguised' PIN was part of a phone number listed in an address book under the same name as the retailer. We could not accept that this was a reasonable attempt to disguise the PIN record or to prevent unauthorised access to the PIN record.

Self-selection of PIN

Rather than keep a PIN record, Financial Ombudsman Service considers that cardholders are far better able to protect the integrity of their accounts if they select their own PIN, where possible, and make their selection a word or string of digits that are so significant to them that no physical record ever needs to be kept.

When choosing a self-selected PIN, cardholders need to take care not to select a PIN that represents their birth date or a recognisable part of their name, as doing so may make them liable for unauthorised transactions. As cardholders typically have more than one card in their wallet, many cardholder's select the same PIN for all their account institution-issued cards. Doing so does not breach any of the requirements of the EFT Code. While having the same self-selected PIN for multiple cards is not a perfect solution to PIN security, as long as that PIN is not voluntarily disclosed to anyone Financial Ombudsman Service considers that it is a preferable strategy to keeping written records of a multiplicity of PINs. Ideally, the self-selected PIN should be constructed in such a way that the cardholder never needs to make a record of it.

Extreme carelessness with security of PIN

Cardholders need to take care that they do not act with extreme carelessness in failing to protect the security of their PINs and passwords. This provision has been part of the EFT Code since 1 April 2002, and was introduced when EFT Code coverage was extended to newer forms of electronic transactions such as phone banking and internet banking. Deciding what would constitute 'extreme carelessness' necessarily involves subjective judgements. The EFT Code attempts to clarify the concept by explaining, in End Note 17 that 'extreme carelessness' means a degree of carelessness with the security of [a PIN or password] which greatly exceeds what would normally be considered careless behaviour. End Note 17 then goes on to give an example of 'extreme carelessness' as being the behaviour of a person who stores their username and password for internet banking in a diary or personal organiser or computer (not locked with a PIN) under the heading "internet banking codes".

Financial Ombudsman Service has only ever used 'extreme carelessness' as a reason for allocating liability to an account holder in circumstances that closely equate to the circumstances instanced in End Note 17. It is difficult to envisage circumstances where 'extreme carelessness' might be relevant to the allocation of liability for a PIN-

authorised card transaction because the EFT Code already has provisions about disclosure, keeping a record of, and self-selection of a PIN. Nevertheless, the very concept of extreme carelessness serves as a reminder to cardholders that keeping their PIN secret and secure is of paramount importance.

The Impact of PIN@POS on Card-Issuing Account Institutions

As noted above, a proportion of credit card transactions have long been covered by the EFT Code. However, until the introduction of PIN@POS, the great majority of credit card transactions were not covered by the EFT Code because they were cardholder-present transactions at merchants that were authorised by signature. Disputes about signature-authorised transactions are considered by Financial Ombudsman Service by reference to the principle of mandate and the Terms and Conditions of the particular credit card product.

Chargebacks

Many disputes about signature-authorised credit card transactions can be handled by the card-issuing institution implementing the chargeback rules of the relevant card scheme, for example Visa or MasterCard. Chargeback rules are formulated by the relevant card scheme, and they govern the interaction between the financial institution that represents the cardholder and the financial institution that represents the merchant. Individual cardholders are not a party to the chargeback rules and have no right to be given a copy of the chargeback rules. However, the existence of the chargeback rules is recognised in the Code of Banking Practice ("CBP") and banks that have adopted the CBP undertake, at clause 20 of the CBP, to:

- Claim a chargeback right where one exists and the cardholder has disputed the transaction within the required time frame;
- Claim the chargeback for the most appropriate reason;
- Not accept a refusal of a chargeback by a merchant's financial institution unless it is consistent with the relevant card scheme rules; and
- Include general information about chargebacks with credit card statements at least once every 12 months.

Disputes about unauthorised PIN@POS transactions will primarily be governed by the provisions of the EFT Code. However, provided that a cardholder notifies a disputed transaction within a time frame that is consistent with card scheme rules and provided that a chargeback right exists, many disputed PIN@POS transactions will continue to be settled by reference to chargeback rules – at least in the first place. The EFT Code recognises this reality in clause 5.11 by providing that:

> *"Where an account holder complains that there is an unauthorised transaction on a credit card account or a charge card account, the account institution shall not hold the account holder liable for losses under clause 5 for an amount greater than the liability the account holder would have to the account institution if the account institution exercised any relevant rights it had under the rules of the*

> *credit card or charge card scheme at the time the complaint was made against other parties to that scheme."*

Where a complaint can be settled using chargeback rules, the EFT Code facilitates this process by allowing, in clause 10.7, that the time frames for resolving a complaint can be extended to time limits that reflect the rules of the relevant card scheme.

One impact that the EFT Code will have on PIN@POS disputes that are lodged within time to chargeback is that clause 5.11 (quoted above) does not require an account institution to exercise a chargeback right. However, End Note 21 to the EFT Code explains that an account institution cannot hold an accountholder liable under clause 5 for a greater amount than would apply if the account institution had exercised its chargeback rights. In other words, if an account institution had a chargeback right but did not exercise it, the account institution could not hold the accountholder liable for the disputed transactions. This principle would apply even if the cardholder had otherwise contributed to the losses within the terms of clause 5 of the EFT Code, such as by keeping an undisguised PIN record with the card in a wallet that was stolen.

<u>No time limits for disputing a transaction</u>

Another impact that the EFT Code will have on PIN@POS disputes is that no time limits can be imposed on account holders to detect unauthorised transactions. This provision is part of clause 4.4, which states in full that:

> *"Account institutions will suggest to account holders that all entries on statements be checked and any apparent error or possible unauthorised transactions be promptly reported to the account institution. This suggestion will be contained on the account statement. Institutions will 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."*

While it is always preferable that an account holder checks their credit card statements on receipt and promptly reports transactions that they consider they did not make, the reality is that many disputes about unauthorised transactions are raised months or even years after the disputed transaction was processed.

As chargeback rights usually remain in place for only three to four months after making a transaction, undue delay in detecting and reporting an unauthorised transaction often means that, by the time a transaction is disputed, the card-issuing institution has lost its ability to reverse the transaction to the merchant's institution. The consequence of losing a chargeback right is that the card-issuing institution has to deal with the issue of allocating liability for unauthorised transactions without being able to offset its potential loss through the chargeback system.

Disputes about the authorisation of signature-authorised credit card transactions are considered by Financial Ombudsman Service with reference to the Terms and Conditions of the particular card facility and general principles of banking law. As many account institutions have Terms and Conditions that require the reporting of unauthorised transactions within a specified time that allows for chargeback mechanisms to be implemented, failure to report within the specified time may mean

that the account holder is held liable for signature-authorised transactions that have not been made by the cardholder. Financial Ombudsman Service accepts that there will be circumstances when an account holder can be held liable for a signature-authorised transaction not made by the cardholder, where the account holder's breach of the time specified for reporting causes the card-issuing institution to suffer a loss caused by the loss of chargeback rights, provided that the relevant provisions of the Terms and Conditions have been brought home to the customer.

There is a full discussion of this issue in the *Policies and Procedures Manual* that was developed by the Banking and Financial Services Ombudsman. An extract from the manual, which contains the sections dealing with Credit Card Disputes and Electronic Funds Transfer ("EFT") Investigations has now been published on the Financial Ombudsman Service website www.fos.org.au in conjunction with this Bulletin. At the 'Publications' button in the top tool bar on the Homepage, choose 'Bulletins', then select 'Banking & Finance Bulletins' to bring up the list of recent and relevant bulletins.

Delayed reporting of PIN@POS transactions

The principles outlined in the extract from the *Policies and Procedures Manual* will not apply to the late reporting of PIN-authorised credit card transactions not made by the cardholder. This is because liability for transactions covered by the EFT Code can only be allocated in accordance with the specific provisions of the EFT Code.

While the EFT Code does have a provision that a cardholder breaches the requirements of the EFT Code if they unreasonably delay notification after becoming aware of the misuse, loss or theft of a card, liability only commences from the time of 'becoming aware' or – in the case of a lost or stolen card – from the time that the cardholder should 'reasonably have become aware'. If a cardholder did not become aware for some months that an unauthorised PIN@POS transaction had been made, for example after a family member had misused the card and returned it to the cardholder, the account holder would not be liable because of that delay for unauthorised transactions that were made before the cardholder became aware. The fact that the card-issuing account institution had lost its right to chargeback the disputed transaction to the merchant's account institution would not be relevant to the allocation of liability because the EFT Code has no provision that links unreasonable delay to loss of chargeback rights.

The practical outcome is that there are likely to be many circumstances where a card-issuing institution will receive a dispute about an unauthorised PIN@POS transaction that has not been lodged in time for a chargeback right to be exercised. It will be important in these circumstances that the card-issuing institution is not unduly influenced by the loss of chargeback rights when it is making a decision about the allocation of liability. Rather, the allocation of liability for unauthorised PIN@POS transactions should always be made by reference to the EFT Code if the unauthorised transaction cannot be charged back.

Transaction limits for PIN@POS transactions

The EFT Code allows that account institutions may apply daily or periodical transaction limits to electronic funds transfers. The EFT Code does not prescribe what those limits

should be, and allows for no limits at all, but it provides that:

1. An account holder's liability for unauthorised transactions will not include amounts that exceed a daily or periodical transaction limit; and

2. An external dispute resolution body may reduce an account holder's liability in certain circumstances if an account institution has not applied a reasonable daily or periodic limit to the transaction.

In clause 2 of the EFT Code, which deals with the availability and disclosure of terms and conditions, there is a requirement at clause 2.3(b) for an account institution to provide information about any restrictions imposed on the use of an access method, including information about daily or periodic transaction limits that apply to the access method, an account or electronic equipment.

The use of a card and PIN to access an account is an 'access method'. There is a comment in End Note 4 that a daily transaction limit may apply to the use of an access method, an account or particular electronic equipment or a combination of these. The ability to construct different transaction limits for different types of electronic equipment means that a range of transaction limits already apply to the use of a card and PIN. For example:

1. The most common transaction limit applied in Australia is to cash withdrawals using card and PIN at an ATM. Each account institution applies their own limit, factoring in issues such as risk, customer expectation and institution objectives. The most common standard limit in Australia is $1,000 per day, but across all account institutions limits range from $800 per day to $3,000 per day. Some account institutions also allow customers to select a higher or lower limit that is subject to institutional approval;

2. Some account institutions apply a different daily limit to card and PIN transactions made at EFTPOS terminals. Thus one daily limit amount could be withdrawn in cash at ATMs and another daily limit amount withdrawn in purchases at merchant EFTPOS terminals;

3. Some account institutions have in-branch PIN-pads installed at teller stations and allow in-branch withdrawals to be authorised by presentation of card and entry of PIN. Typically, these account institutions apply no specific limit to in-branch withdrawals and allow withdrawals up to the available balance of an account. Depending on the amount withdrawn, these account institutions may require additional identifying information to be produced (such as photo ID) in addition to entry of correct PIN, in order to ensure that the person making the transaction is the true cardholder.

It can be seen from the above that there are a number of existing daily transaction limits applying to transactions made with a card and PIN, ranging from about $800 per day to no limit at all subject only to the available balance of an account.

A survey of member banks made by Financial Ombudsman Service since the introduction of PIN@POS indicates that most PIN@POS transactions made on a credit card account will either have no limit at all (subject to the available credit of an account) or a high

capped limit (e.g. $25,000 per day). The rationale for setting limits in this way seems to include factors such as:

1. Under the signature-authorised regime, a cardholder could use their credit card at a merchant to make a transaction that fully utilised the available credit of the credit card account (subject to authorisation by the account institution that issued the card);

2. Cardholders would have an expectation that there should be no differentiation between the type and amount of a transaction that could be authorised by signature and the type and amount of a transaction that was authorised by PIN;

3. It would hinder the take-up of PIN@POS by cardholders and merchants if PIN-authorised transactions were subject to a lower limit than applied to signature-authorised transactions.

It must be said at the outset that setting no daily limit or a very high daily limit for PIN@POS transactions does not breach any of the requirements of the EFT Code. The ability, as mentioned above, to vary limits according to a combination of access method, account and electronic equipment means that transactions on a credit card account can have completely different limits (including no limit) compared to transactions on a savings or cheque account, and transactions with a credit card can have different limits to transactions with a debit card.

However, setting no limit or a very high limit for PIN@POS transactions increases the risk of loss to the account institution that sets those limits. More importantly, from the perspective of the EFT Code, no or high limits expose an account holder to greatly increased liability for losses resulting from unauthorised PIN@POS transactions where the cardholder has breached one of the requirements of the EFT Code, for example by disclosing the PIN to the person who made the unauthorised transactions.

Financial Ombudsman Service will have regard to the provisions of clause 5.12 of the EFT Code when considering disputes about the allocation of liability for unauthorised PIN@POS transactions. Clause 5.12 was introduced with effect from 1 April 2002. It was introduced at the same time as account institutions were given the ability to vary transaction limits according to access method, account and electronic equipment. In effect, clause 5.12 recognises that the 'freeing up' of transaction limits introduced benefits for both account institutions and customers when transactions were validly authorised, but increased the potential liability for account holders when transactions were unauthorised. Clause 5.12 then can be seen as a type of countervailing provision that requires account institutions to give up some of the benefits of transaction limit flexibility in order to limit the impact on account holders of unauthorised transactions.

Clause 5.12 of the EFT Code introduces a discretion to reduce an account holder's liability for an unauthorised transaction where no reasonable daily or periodic transaction limit applies to the transaction. The discretion can be exercised by either the account institution or by an external dispute resolution body such as Financial Ombudsman Service.

The circumstances in which the clause 5.12 discretion would apply are as follows:

1. There is an unauthorised transaction and the account institution has not applied a reasonable daily or periodic transaction limit. The clause then specifies that the reasonableness of a transaction limit is to be determined having regard to prevailing industry practice;

2. The security and reliability of the means used by the account institution to verify that the relevant transaction was authorised by the user [the cardholder in the case of PIN@POS] did not adequately protect the account holder from losses in the absence of the protection afforded by a reasonable daily or periodical limit;

3. Where the transaction involves drawing on a line of credit [which would include a PIN@POS transaction on a credit card account], the account institution had not taken reasonable steps, at the time of making the line of credit accessible by the access method, to warn the account holder of the risk of the access method being used to make unauthorised transactions on that line of credit;

4. Where the above circumstances apply, the account institution or an external dispute resolution body may reduce any liability that the account holder has for unauthorised transactions by such amount as they consider fair and reasonable.

Although it has not happened very often, there have been circumstances in which Financial Ombudsman Service has resolved a dispute by invoking the discretion granted by clause 5.12 of the EFT Code. The type of circumstance can be illustrated by the following examples that have been based on actual disputes: the first where there are in-branch withdrawals authorised by PIN at the teller PIN-pad, and the second where high value merchant transactions are made possible by a separate daily limit applying to card and PIN transactions at a merchant EFTPOS terminal.

Dispute involving in-branch withdrawals

A thief stole a debit card and gained knowledge of the PIN from a record kept with the card. The thief then withdrew $9,000 in a single branch transaction, authorised by presenting the card to the teller and inputting the PIN at the teller station PIN-pad.

The account institution applied a limit of $1,000 per day to card and PIN withdrawals at an ATM. However, it allowed in-branch withdrawals up to the balance of the account. The procedure that tellers were required to observe was that withdrawals of $10,000 and above had to be accompanied by the production of photo ID that was sufficient to verify that the person presenting the card was the actual cardholder. However no additional identification, apart from card and entry of correct PIN, was required for withdrawals under $10,000.

Taking into account the usual daily limits that applied across the banking industry to card and PIN withdrawals at ATMs, Financial Ombudsman Service considered that the lack of a limit for in-branch withdrawals meant that no reasonable daily limit applied; and the fact that no additional identification steps were in place for withdrawals under

$10,000 meant that the account holder was not adequately protected from losses in the absence of a reasonable daily limit.

Financial Ombudsman Service acknowledged that the cardholder had contributed to the losses by keeping a record of the PIN with the card, but reduced the account holder's liability to $1,000 – which was the daily limit for ATM withdrawals at the particular account institution - in accordance with the discretion granted by clause 5.12.

Dispute involving separate EFTPOS limit

A thief stole a debit card and gained knowledge of the PIN in circumstances that were not clear. The account institution that issued the card applied a daily limit of $1,000 to cash withdrawals at ATMs but applied a separate daily limit of $8,000 to EFTPOS transactions at merchants. The account holder was unaware that his card had a separate limit for EFTPOS transactions because the EFTPOS limit was not adequately disclosed and publicised by the account institution at the time. However the existence of the EFTPOS limit had become known to the thief who purchased high value electronic equipment to the value of $40,000 over a five day period before the cardholder became aware that his card was missing.

Financial Ombudsman Service surveyed a number of member account institutions about the limits that might apply to EFTPOS transactions and concluded that $8,000 was not a reasonable daily limit having regard to prevailing industry practice. As the merchant required no authorisation apart from production of the card and entry of correct PIN, we also concluded that there were no secure and reliable means in place to protect the account holder from losses in the absence of a reasonable daily limit. Without reaching a decision about whether the cardholder had contributed to the losses, we suggested to the account institution that it should reimburse the account holder in full. The account institution accepted our viewpoint and refunded the $40,000 in dispute without a formal Finding being prepared.

<u>What is the likely impact of clause 5.12 on disputed PIN@POS transactions?</u>

The fact that most account institutions have indicated that they will not apply any transaction limit (up to the amount of the available credit) to PIN@POS transactions means that there is a potential for a significant increase in account holder liability for unauthorised PIN@POS transactions.

In the first place, account institutions should inform their account holders about the transaction limits, or lack of transaction limits, that will apply to PIN@POS transactions. This is because there is a requirement in clause 3 of the EFT Code that account institutions provide written notification to account holders when the account institution wishes to vary or modify the EFT Terms and Conditions to impose, remove or adjust a daily transactions limit or other periodic transaction limit that applies to the use of an access method, an account or electronic equipment. In addition, account institutions are specifically required to give clear and prominent advice to account holders that the removal of or an increase in a transaction limit may increase account holder liability in the case of unauthorised transactions.

When considering a dispute about liability for unauthorised PIN@POS credit card transactions, Financial Ombudsman Service will consider whether or not it would be appropriate to reduce an account holder's liability in accordance with clause 5.12 after taking into account the factors summarised above, namely the reasonableness of the transaction limit having regard to prevailing industry practice, whether the means of verification that the transaction was authorised by the cardholder adequately protected the account holder from losses, and whether the account institution had taken reasonable steps to warn the account holder of the risk arising from unauthorised transactions.

Financial Ombudsman Service, as always, will consider any disputes that arise in future in relation to the particular circumstances that apply to an individual dispute.

Transactions that exceed the credit limit of a credit account

Another area where the EFT Code has the potential to impact on unauthorised PIN@POS transactions is where unauthorised transactions cause the agreed credit limit of a credit card account to be exceeded. This could occur, for example, where transactions that are less than a merchant's floor limit are processed to the credit account without a check being made that sufficient credit is available for the transaction.

Irrespective of whether or not the cardholder contributed to the losses resulting from unauthorised PIN@POS transactions by contravening any of the requirements of the EFT Code, the EFT Code provides that the account holder cannot be held liable for unauthorised transactions that exceed the agreed credit limit of the account. The relevant clause of the EFT Code that brings about this outcome is clause 5.5(a)(iii), which provides that the account holder is not liable for amounts that exceed the balance of the account (including any prearranged credit). There is a similar provision in clause 5.5(b)(iii), which deals with losses arising out of unreasonable delay in notification.

Financial Ombudsman Service routinely assesses all EFT Code-related disputes to ensure that any losses for which an account holder might be liable do not exceed the balance of an account or the prearranged credit limit of an account.

The Impact of the EFT Code on MOTO Transactions

Some credit card transactions are conventionally referred to as 'MOTO' transactions, the abbreviation being derived from 'mail order and telephone order'. These days, MOTO transactions include transactions made over the internet. In simple terms, a MOTO transaction is one where the cardholder is not present at the merchant when the transaction is processed. Mail order transactions would not be covered by the EFT Code where the cardholder had signed the order to debit the account, however transactions initiated by phone or internet would come within coverage of the EFT Code.

There is no doubt that MOTO transactions provide great benefits to cardholder, account holders, merchants and the account institutions that issue cards and process transactions. Without MOTO there would be no ability to pay utility bills over the phone or internet and no ability to order and pay for goods and services over the phone or internet, just to give a couple of examples.

However, MOTO transactions constitute a risk for everyone involved in the credit card system because there is no conventional authorisation by either signature or PIN on the part of the cardholder. All that is needed to process a MOTO transaction is knowledge of the card number, knowledge of the expiry date and, in some but not all instances, knowledge of the 3-digit 'card verification value' ("CVV") that is printed on the reverse of a credit card. These three pieces of information are categorised as "identifiers" in the EFT Code. There is no requirement in the EFT Code for identifiers to be kept secret. The non-secret nature of these identifiers is evident from the fact that they appear on the card itself, are routinely communicated to merchants and are accessible from account institution data bases. Anyone who gains knowledge of card number and expiry date can attempt to charge a transaction to an account holder's account. Some merchants will also ask for the CVV to be quoted, which may reduce the risk of an unauthorised transaction being processed where the perpetrator has not sighted or does not possess the actual credit card, but not all merchants follow such a procedure.

MOTO transactions can be initiated by anyone who has gained knowledge of the card identifiers, without any conventional authorisation by the card holder and without the cardholder breaching any of the specific requirements of the EFT Code. There are no requirements in the EFT Code to keep identifiers secret, and account holders have no control over the misuse of identifiers by merchants or the inadvertent release of identifier information from merchant or account institution data bases.

The approach that the EFT Code takes to unauthorised MOTO transactions by phone or internet, where possession of the physical card is not needed to initiate the transaction, is to have no provision at all within the EFT Code that would allow an account institution to allocate liability for an unauthorised phone or internet MOTO transaction to the account holder. While this approach is 'negative' rather than being positively spelt out in the EFT Code, the no-liability-approach can be constructed from the following provisions:

1. The liability provisions of clause 5.6 of the EFT Code, including liability where the user [that is, the cardholder] acts with extreme carelessness, only apply where the access method utilises a code or codes [that is, a PIN or password]. As no account-institution-issued PIN or password is usually required for a MOTO transaction, the provisions of clause 5.6 do not usually apply to MOTO transactions;

2. Clause 5.5(c), which limits an account holder's liability to $150 in circumstances where the account institution has not proved on the balance of probability that the user contributed to losses, is also only applicable where a code is required to perform the unauthorised transaction;

3. The remaining method by which a user can contribute to losses is by unreasonable delaying notification after becoming aware of the misuse, loss or theft of a device, which is set out in clause 5.5(b). In terms of a MOTO transaction, the 'device' is the credit card. However, the wording of clause 5.5(b) requires that the device or card form part of the access method. The definition of 'device' in clause 1.5, which is that 'device' means a physical device used with electronic equipment to access an EFT account, further clarifies that unreasonable delay will only apply in circumstances where there is physical

> interaction between the card and electronic equipment. As MOTO transactions only require knowledge of the identifiers pertinent to the card rather than the card itself, and as the card itself does not interact with electronic equipment when the identifiers are being quoted, it can be seen that the unreasonable delay clause will not usually apply to MOTO transactions.

Effectively, then, there are no provisions in the EFT Code that allow an account institution to allocate liability for unauthorised MOTO transactions to the account holder. While this reality is not spelt out positively in the EFT Code itself, there is a mention of it in End Note 4 to the EFT Code, which includes (among other things) the following comments:

> *'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 (eg. use of a credit card number through a 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* [that is, PIN or password] *or a device (see sub-clauses 5.5 and 5.6). 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 the loss or theft of the device (see paragraph 5.5(b)).'*

As a final comment, an example of the use of a device without a code – where unreasonable delay could apply – is use of a credit card to gain entry to a carpark where a second insertion of the card at the exit point, without entry of a PIN, is sufficient to generate a debit to the credit card account. In this example it is important to note that, while there is no conventional authorisation by PIN or signature, the physical card interacts with the electronic equipment that reads the card details at entry and exit.

Further Information

Financial Ombudsman Service has published a number of references to the resolution of disputes involving the EFT Code. All are accessible from the Financial Ombudsman Service website www.fos.org.au by selecting the 'Publications' button on the Home Page and then selecting 'Bulletins' and 'Banking & Finance Bulletins'. If you are viewing this Bulletin online you can also access the documents directly using the links provided.

The references include:

- The extract from the Policies and Procedures Manual dealing with credit card disputes and EFT investigations;
- Bulletin 49, March 2006, which includes a Finding about an EFT Code-related dispute;
- Bulletin 40, December 2003, which includes commentary about online and offline credit card fraud;

- The Supplement to Bulletin 39, September 2003, which includes commentary about emerging issues in electronic banking;

- Bulletin 37, March 2003, which includes commentary about conducting investigations into EFT Code complaints;

- Bulletin 35 and the Appendix, September 2002, which includes commentary on emerging issues in electronic banking and a detailed commentary on what was then the newly revised EFT Code.

Anyone wishing to discuss the approach that the Banking & Finance division of Financial Ombudsman Service takes to EFT disputes can contact Laurence O'Keefe, EFT Disputes Manager, by phone on 03 9613 7326 or 1300 780 808 or by email to lokeefe@fos.org.au

As is always the case, we welcome feedback on this Bulletin.

Philip Field
Ombudsman – Banking & Finance
Financial Ombudsman Service