RECENT DEVELOPMENTS NO. 2
EFTPOS - AN UPDATE

S.A. LANCASTER

Senior Corporate Solicitor
Australia and New Zealand Banking Group Limited

First I should say that the opinions expressed in this paper are my personal opinions and are not necessarily the view of my employer.

1. WHAT IS EFTPOS?

EFTPOS is but one application in the Electronic Funds Transfer (EFT) system which has blossomed in Australia over recent years and of which the now familiar Automatic Teller is the most visible and most accepted application.

EFTPOS of course is an EFT application in which the electronic funds transfer (EFT) is initiated at the point of sale (POS).

EFTPOS is not a new payment system. We have had in place for many years a payment system which allows for the transfer of value by debiting one bank account and crediting another. This same payment system is also used in connection with EFTPOS transactions, the difference being that with EFTPOS the transaction is effected via electronic messages rather than via written instructions on pieces of paper (cheques, travellers cheques, credit card sales). EFTPOS then is a term for describing ways of processing transactions in the existing payments system.

There are two types of message involved in an EFTPOS transaction, being (1) the message to authorise the transfer of funds and (2) the message that actually transfers the funds.

These are illustrated in the diagram below:

EFTPOS TERMINAL Customer (Card & PIN)

(1) Customer's instructions to debit account provided funds are available

CUSTOMER'S ACCOUNT

(2) Transfer to Merchant's Account

MERCHANT'S ACCOUNT

Note (1) Instruction is irrevocable - see Conditions of Use
(2) Debit is immediate
(3) Time delay in crediting Merchant's Account

2. EFTPOS ACCEPTANCE IN AUSTRALIA

EFTPOS was introduced in Australia in 1984 by way of pilot schemes.

There are now close to 4,000 terminals in operation, about half of these being in service stations, but it is still true to say that EFTPOS in Australia is still very much an infant and even those networks which are running are pilot or advanced pilot schemes. Nevertheless there is great potential, particularly considering Australians' demonstrated willingness to embrace new electronic technology in their financial dealings. NCR Australia Pty Ltd has estimated the market potential as 50,000 shopfront terminals by 1990, but other much higher estimates have been made. (Source - Financial Services Report Jan/Feb 1986.)

At this stage the major outlets are the large petrol distributors, B.P., Mobil, Shell, Caltex, Ampol and large chainstores Coles-Myer, Woolworths, Food Plus, Safeway, K Mart and also the Dick Smith electronics stores. There are also some specialised applications such as TAB, Electricity Commissions of Queensland and Western Australia.

3. GOVERNMENT ACTION

There has been a great deal of public debate concerning the contractual conditions imposed by issuing institutions on their card holder customers in connection with EFT transactions.

This has led to action on two fronts. First, the setting up by the Federal Government of a working group to examine the rights and obligations of the users and providers of electronic funds

transfer systems and, secondly, an initiative by the Standing Committee of Consumer Affairs Ministers (SCOCAM) in preparing a code of practice for the operation of EFTs.

In June, 1984 the Federal Government announced the formation of Working Group under the chairmanship of the Commonwealth Treasury to examine consumer aspects of EFT systems.

The Working Group was comprised of representatives from the following Commonwealth Departments and organizations:

- Treasury (Chair)
- Reserve Bank of Australia
- Attorney-Generals
- Prime Minister & Cabinet
- Industry, Technology and Commerce
- Communications
- Home Affairs and Environment
- Telecom Australia

The Working Group reported in December, 1985 and significantly the report favoured industry self regulation rather than legislative regulation to bring about various changes which it recommended.

However, the recommendations, which are summarised in section 6.2 of the Report include the following:

- The Working Group believes it would be desirable for the Group to be reconvened within approximately six months of the public release of the Group's Report to report to Ministers on the progress achieved in relation to the Group's proposals.

- The Working Group recommends that the Treasurer, the Attorney-General and other relevant Commonwealth Ministers assess the situation in, say, two years to determine whether a further examination of the need for more formal arrangements relating to consumer interests in EFT is warranted.

The State Governments, through the Standing Committee of Consumer Affairs Ministers, resolved to prepare a code of practice and this was released in January, 1986. This SCOCAM Code, a copy of which is attached, is comprehensive and detailed.

Although the Code is intended to be voluntary, the States have made it clear that if it is not adhered to, consideration would be given to introducing legislation along similar lines.

The report of the Working Group and the code of practice are the most significant regulatory developments in this area and will provide the main focus for discussion today.

Most of the concerns with issuing institutions' Conditions of Use centred on two areas.

1. Risk Allocation (i.e. when things go wrong, who bears the loss - card issuer or card holder?).

2. Error Resolution (i.e. how to resolve disputes between the card issuer and the card holder).

Today Dr Chin Yen Lee will deal with Error Resolution and also generally the report of the Working Group referred to earlier. For my part I will concentrate on Risk Allocation and generally the SCOCAM Code of Practice.

4. RISK ALLOCATION

The main problems which have been encountered with EFT have been:

- Many conditions of use do not have any monetary limit on losses which the cardholder might have to bear.

- On occasions the account was permitted to overdraw thus giving rise to losses in excess of the balance in the account.

- Daily/weekly transaction limits imposed on the cardholder were permitted to be exceeded, again giving rise to losses in excess of what the cardholder might reasonably have believed possible.

The last two of these are generally associated with an ATM being "off-host", meaning that it is not directly connected to the main or host computer at the time.

Another concern relates to consequential losses. Issuing institutions have generally sought to exclude liability for consequential losses.

The Working Group in its Report recommended that:

- Financial institutions should make it clear in their contracts that under circumstances of unauthorised access to an account, the cardholder will not incur liability for an amount greater than the account balance or credit limit.

- Financial institutions should accept in their contracts an obligation which limits a customer's daily liability in cases of unauthorised use of a card to the daily transaction limit.

- In cases of technical malfunction the financial institutions should amend the clause in their Conditions of Use dealing with technical malfunction to set out more clearly the rights and obligations of the financial institutions and their customers. Financial institutions should set out the

exact circumstances for which they will, or alternatively will not, accept liability so that customers know precisely what their rights are and can make informed decisions about use of EFT systems.

I now propose to refer to the SCOCAM Code of Practice, in particular clause 7 which is headed "Liability of cardholders for unauthorised transfers". Refer to the Code of Practice for the actual provisions under the various sub-headings. It will be seen that clause 7 tackles all of the problems mentioned above which have been encountered with EFT.

Clause 7.1 Losses caused by the misuse by third persons of a lost or stolen card

This proposes a two tiered level of responsibility depending on whether or not the cardholder may have contributed to the loss caused by the misuse in certain specified ways.

If the cardholder is innocent then his maximum risk is $50.00.

If the balance of the account (including pre-arranged credit) is less than $50.00, then his risk is correspondingly reduced.

Furthermore the financial institution is responsible for all unauthorised transactions occurring after the time of notification of the loss or theft of the card.

If the cardholder may have contributed to the loss in any of the specified ways his maximum risk is increased to $250.00 but again limited by the balance of the account including pre-arranged credit. It is further limited by daily/weekly transaction limits applicable to the cardholder up to the time of notification and the financial institution is responsible for unauthorised transactions occurring after the time of notification of the loss or theft of the card.

Comment

(i) "balance of the account"

The potential loss of cardholder is, in part, limited to the balance of the account. It seems to me that this must be taken to mean the balance in the account from time to time over the relevant period as distinct from, say, the balance in the account at the time of the loss of the card.

(ii) "including any pre-arranged credit"

The inclusion of credit lines available on the account is clearly necessary but the requirement for it to be pre-arranged could provide some problems, probably unintended, where the account being accessed is a cheque account with a bank. It is common for customers to draw cheques for amounts in excess of credit balances or approved overdraft limits and, contrary to popular

opinion, the bank manager will usually honour those cheques (thus creating an overdraft or an excess of limit), if he is satisfied that the customer is creditworthy, and he might record a limit arrangement for internal purposes.

Although a cheque drawn by a customer whose account does not hold sufficient balance to meet it, constitutes a request to the bank to advance the relevant amount to the customer (Cuthbert v. Robarts, Lubbock & Co (1909) 2 Ch. 226) it could hardly be said that this internal limit gives the overdraft the status of "pre-arranged credit".

(iii) "may have contributed to the loss"

The higher level of customer risk applies where the cardholder may have contributed to the loss in the ways stipulated.

On the literal reading the higher limit might be thought to apply on the basis that having voluntarily disclosed the PIN, or having written the PIN on the card, etc. that action raises the possibility that the cardholder contributed to the loss. However clause 12.7 makes it clear that the act alone does not make the higher level applicable.

It provides that financial institutions should not seek to avoid liability on the basis of conduct by the cardholder which is in breach of contract, if that conduct does not relate directly to the cause of the loss and cannot be shown by the institution to have contributed to the loss.

(iv) "keeping a copy of the PIN in uncoded form with the card"

This is one example of conduct by the cardholder which can cause the higher risk level to apply. It carries with it the implication that if the PIN is carried with the card in coded form then the lower risk level will apply.

It is submitted that coded records might be so elementary as to offer no protection at all. For example suppose a record was kept with the card in the following form:

" A B C D E F G H I J
1 3 2 4 "

Any schoolboy would be able to deduce that the PIN was 2639.

Query also whether a simple reversal of the PIN numbers would be regarded as being coded or uncoded in form. Whatever it is, it would be dangerous and irresponsible for a cardholder to record his PIN in this manner and carry the record with his card.

(v) "discovering the loss or theft"

Delay in advising the financial institution after discovering the loss or theft can also cause the higher risk level to apply.

It seems to me that there are some situations in which even though the cardholder does not have actual knowledge of loss or theft, it would not be unreasonable to expect the cardholder to take some steps to check the security of his card. For example if his house has been burglarised.

Clause 7.2 Misuse by agents acting beyond their authority

This provides that where a cardholder has intentionally disclosed the PIN to a third person and allowed that person to use the card to withdraw money or to transfer funds, the cardholder shall be responsible for all transactions occurring while that person is in possession of the card with the cardholder's consent.

Comment

(i) Financial institutions are likely to find this clause absolutely unacceptable in that it impliedly countenances the practice of a cardholder authorising another person to use his card.

I believe that most financial institutions are totally opposed to a cardholder disclosing his PIN and delivering his card to a third party for any reason whatsoever and that this is made a contractual condition. If they became aware that the PIN had been disclosed I believe they would insist on issuing a new PIN.

I submit that this provision can only be seen as encouraging and sanctioning a practice which has nothing to recommend it. EFT transactions rely heavily on the security of the PIN and this security depends largely on it being confidential to the cardholder. The moment the cardholder discloses the PIN to another that security is broken.

(ii) Curiously if the cardholder discloses his PIN and gives his card to another to obtain a balance of account or make a deposit to the account the clause does not operate even though by withdrawing funds the agent would be acting beyond authority. Further, clause 7.1 would have no application because it is only concerned with lost or stolen cards.

(iii) A further curious feature is that the cardholder is only responsible for transactions occurring while that person is in possession of the card with the cardholder's consent.

Thus if the cardholder advises the agent that his authority is terminated but the agent fails to return the card upon request then clearly he no longer holds that card with the cardholder's consent and presumably the cardholder is no longer responsible for unauthorised transactions, according to clause 7.2.

Again clause 7.1 is not applicable because the card is not lost or stolen.

Clause 7.3 Counterfeit, faulty, cancelled, expired or improperly issued cards

All losses relating to cards of this description shall be the responsibility of the financial institution.

Clause 7.4 Machinery/software related losses

As between a cardholder and the issuing institution any losses relating to or caused by faults in EFT machinery or computer software, shall be the responsibility of the institution. An inclusive definition of "fault" is included.

Comment

(i) I have no argument regarding losses caused by faults in EFT machinery or computer software. Presumably the addition of the words "relation to" are intended to widen the operation of the clause but their practical effect is not clear to me.

It seems to me that "caused by" is as far as the protection needs to extend and the words "relating to" should be deleted.

(ii) Definition of "fault"

It seems to me to be totally unnecessary to include the first three points of this definition unless it is thought that a "failure" is not a "fault". If that be the case a simpler solution would be to refer to "faults and failures" in the opening words rather than simply "faults". As to the final point (inadequate security permitting unauthorised access and enabling unauthorised transfers from accounts) one wonders if it needs to be said. It seems to be directed at the "hacker" situation but I can't imagine any issuing institution seeking to place this risk on the cardholder.

Clause 7.5 Off-line losses

As between the cardholder and the issuing institution losses which are due to either the EFT terminal being off-line or through it not functioning correctly shall be the responsibility of the institution.

Comment

I see no objection to this provision in principle but it seems to be unnecessary. I cannot identify losses under this heading which would not otherwise be covered.

Clause 7.6 Losses caused by insiders

As between the cardholder and the issuing institution losses attributable to the fraud or negligence of employees of the issuing institution or merchants, shall be the responsibility of the issuing institution.

Clause 7.7 Liability for consequential losses

Financial institutions are to be liable for all losses that are reasonably foreseeable and shall not attempt to limit their liability to cardholders or customers to direct losses only.

Comment

This provision is one of the most controversial in the Code. Issuing institutions wish to have the right to limit their liability to direct losses only.

Provided the limitation is clearly spelt out in the conditions I believe that issuing institutions should be free to limit their liability. This is a matter that will affect pricing and it is not as though there is any lack of competition in the market place.

It is sometimes argued by those who favour a ban on limitation clauses that if the cardholder paid by cheque he would be entitled to consequential losses for wrongful dishonour and therefore should be in the same position with EFT. This is a spurious argument. The short answer to it is that if the person concerned requires that extra recourse he can pay by cheque. It is usually not so convenient but that is a trade-off for the additional recourse. EFT and cheques are different products for payments just the same as a Range Rover and a Jaguar Saloon are different products of motor vehicles. They each have advantages and disadvantages compared to each other and the user should choose the appropriate product for his particular requirement. I hope he would not drive his Jaguar along rough mountain tracks.

FURTHER COMMENT ON THE SCOCAM CODE OF CONDUCT

1. Clause 1.1 sets out the types of transactions to which the guidelines apply and clause 1.2 sets out certain transactions to which they do not apply.

Comments

(i) They apply to pre-arranged automatic transfers of funds from customer accounts. This appears to mean what are commonly called periodical payments, i.e. transfers made from an account under a standing authority from the customer on pre-arranged dates or at pre-arranged intervals. This service has been provided by banks for as long as I can remember and certainly long before EFT was dreamed of. It has historically been paper based but naturally banks and other financial institutions have utilised their electronic systems to make the payments. The term also appears to include "sweep arrangements", i.e., arrangements for a financial institution to transfer or sweep balances between accounts when they reach certain pre-determined levels, so as to maximise interest earned or minimise interest paid. Plastic cards and PINs are not involved in either periodical payment or

sweep arrangements and I believe they should not be included in the guidelines.

(ii) They do not apply to "automatic transfers of funds to customer accounts". Presumably this includes direct payroll crediting.

(iii) "Funds transfers made at a branch or office of any financial institution for a customer of that institution by an employee of the institution" are excluded.

This appears to exempt all "over the counter" transactions at a branch.

2. Clause 2.1 dealing with unsolicited cards appears to be unnecessary in view of section 63A of the Trade Practices Act and proposed amendments to cover debit cards.

3. Clause 3.3(iv) requires disclosure in the terms and conditions of "a description of transactions" that may be made with the EFT card, including details of accounts from which withdrawals or transfer can be made and any lines of credit which can be drawn against.

Comment

This requirement is misconceived. The customer makes separate arrangements with the issuing institution from time to time regarding which accounts he wishes to be accessed. Lines of credit are subject to separate arrangements and are not part of the EFT system.

4. Clause 3.3(vi) requires disclosure in the terms and conditions of details of standard bank charges where an account is overdrawn.

Comment

This requirement is also misconceived. The charge referred to relates to the operation of the account accessed, not to the EFT transaction itself.

5. Clause 4.2 requires the financial institution to send a statement of account to the customer monthly (unless the customer requests a different frequency) and stipulates information to be included on the statement.

Comment

There appears to be no compelling reason to make it mandatory to send out statements monthly; that should properly be left to the financial institution and its customer.

Monthly statements would entail a significant cost which ultimately would be passed on to the customer.

6. Clause 5.1 provides that the customer shall be entitled to certain information in relation to accounts which can be accessed through an electronic terminal using an EFT card. This information includes "a copy of the current terms and conditions relating to the account ...".

Comment

This is one of several examples in the Guidelines of a failure on the part of their author to grasp the distinction between the account being accessed and the EFT system.

To comply with such a request in relation to a cheque account might a bank have to provide the account opening and operating authorities and copies of Paget's Banking Law and Weaver and Craigie's Banker & Customer in Australia plus numerous assorted law reports?

7. Clause 12(3) provides that financial institutions shall not seek to promote the use of electronic funds transfers methods in preference to other payment methods by imposing higher charges on customers using such other methods.

Comments

Presumably this is directed at banks and their cheque facilities.

Banks should be free to determine the charges on any payment system and, if it suits its particular business strategy, even price its systems so as to make one more attractive than the other. If that bank gets its prices and strategies wrong, it will pay the penalty in the market place.

8. 12.6 Prohibition of certain terms in contracts. This clause sets out six separate terms which are not to be included in contracts relating to the use of EFT services or EFT cards.

(i) Terms imposing liability on customers other than in accordance with these guidelines.

Comment

This seems to indicate an intention to require issuing institutions to formally agree to observe the guidelines.

(ii) Terms "deeming" customers to have accepted the accuracy of statements concerning their accounts if no objections are raised within a certain period after receipt of a periodic statement.

Comment

In my opinion it is not at all unreasonable to require a person receiving a statement of his account to check that statement and to have a limited but reasonable time in which to advise the issuer of disputed transactions.

It was put to me by one of the Victorian officers involved in drafting the Code of Practice that this provision is in line with the recent decision in Tai Hing Cotton Mill Ltd v. Liu Chong Hing Bank Ltd (1985) IBL 71, but that is not so. Certainly that case settled the point that a bank customer's duty of care which he owes to his bank does not extend to checking his bank statement for accuracy. However it is altogether another matter to say to the banks that they are not to be permitted to contract with their customers on terms which do impose such a duty on the customers. In fact that point was specifically recognised by their Lordships in Tai Hing Cotton.

It would not surprise me at all if some Australian banks do take this path in the future.

Incidentally in the USA a cardholder has 60 days in which to report any unauthorised transactions included in a periodic statement, failing which he incurs unlimited liability for further transfers occurring after the 60 days.

(iii) Terms making it a prerequisite to the commencement of any legal proceedings concerning a matter in dispute for that matter to be referred to arbitration.

(iv) Terms "deeming" notices to have been received by customers or cardholders where those notices have not actually been delivered or sent to those customers.

Comment

While acknowledging that there may be an element of commercial expediency in such deeming provisions there is a much larger element of commercial necessity.

Short of registered or certified mail which is cost prohibitive or personal delivery which is quite impractical a financial institution would hardly even be able to prove receipt by the cardholder.

(v) Terms limiting liability for losses in relation to a disputed transfer or payment to the amount of that transfer or payment.

Comment

As with clause 7.7 it should be left to the individual financial institutions to determine their respective policies on this question. The price paid for the service will reflect the risk assumed and consumers have a wide choice of card issuers and also a wide choice of methods of payment.

9. 12.7 Non-causative exemptions. This clause provides that financial institutions should not attempt to avoid liability for losses where although the customer or cardholder is in breach of contract, that breach did not relate directly to

the cause of the loss and cannot be shown by the institution to have contributed to the loss.

Comment

My concern here is only with the onus of proof being placed on the institution to show that the breach caused the loss.

To take an example, suppose cardholder C disclosed his PIN to X. Without C's knowledge X disclosed the PIN to Y. Y, a resident of the same household as C and X, stole C's card and withdrew moneys from his account. Although C's disclosure of the PIN would presumably relate directly to the cause of the loss it would be impossible for the financial institution to show that it contributed to the loss.

I submit that the words "and cannot be shown by the institution to have contributed to the loss" should be deleted.

12.6 Networking arrangements. This clause makes it clear that as between an issuing institution and its customer, the issuing institution is responsible for losses caused by other financial institutions with which it has networking arrangements.

STATUS OF CODE OF PRACTICE

Unless incorporated into the contract by reference or unless actionable in particular circumstances as a collateral warranty, then clearly the Code of Practice would have no contractual force between the issuing institution and the cardholder.

However if the issuing institution represented that it complied with the Code of Practice but did not in fact, and if its terms and conditions were inconsistent with the Code of Practice these matters could constitute "misleading and deceptive conduct" within the meaning of section 52 of the Trade Practices Act and attract the wide remedies available under that Act.

Whatever the legal status may be an issuing institution is hardly likely to deliberately flout a Code to which it had indicated its approval. The forces of consumerism through Government Consumer Affairs Departments, the media through radio talk-back programmes and television programmes such as the ABC's "The Investigators", not to mention crusading politicians, would make that a foolish policy indeed. I have emphasised the word "deliberately". Unless the Code is expressed in unambiguous language there is a danger that an issuing institution may unwittingly transgress.

In my opinion the authors of the SCOCAM Code of Practice have gone into far more detail than is desirable in a document of this nature. It is drafted more as a legal document attempting to cover with particularity every detail.

Nevertheless the SCOCAM Code of Practice is a valuable document. It does identify the important issues even if, as I believe, in tackling those issues it goes further than is necessary or desirable in some respects.

Hopefully there will be some re-assessment and, given good will on both sides, I believe that a very useful and important document will be accepted by all concerned.