Electronic Funds Transfer Systems Practice and the Law

Comment by

Dr. C. Y. Lee

Senior Lecturer in Law
Monash University

I think Mr. Douglas' definition of E.F.T. as the use of telecommunications to transmit financial data in computer readable form, from point to point, from payer to receiver, without the need for supplementary paper documents to support the transaction, is as good as any that I have seen.

The American authors, Katskee & Wright, have defined E.F.T.S. to be 'a process of value exchange achieved through the use of electronic devices', the value exchange being brought about by debit or credit orders. Essentially it is about the transfer of money and it is part of the payments system. But then Mr. Douglas went on to say that E.F.T.S. has no direct effect on the evolved arrangements between banker and customer and that it leaves intact traditional formal arrangements concerning liability, confidentiality, privacy and the banker-customer relationship. To a large extent, that is true, but the inherent characteristics of E.F.T.S. dictate that we re-examine these traditional arrangements and relationships, and consider if there is a need for legislation.

My brief has been to comment on the paper with regard to the consumer, whom I will take, for the purposes of the discussion, to include all users, including corporations, who initiate an E.F.T. transaction. My belief is that government involvement will not be relegated to concerns arising from the effectiveness of the exchange of value system and control of monetary policy. It should, and ought to, look at legitimate consumer concerns arising from the nature of an E.F.T. transaction.

First, let me identify a few of the E.F.T.S. characteristics.

1. A significant attribute is the reduction in the amount of paper.
2. The transaction is almost instantaneous.
3. The signature which is used to authorise and authenticate paper transactions is replaced by personal identification numbers, test keys and other identifying codes.
4. Computers are machines, and are subject to breakdowns, errors and 'downtime'.
5. Information has to be fed into the computer, and with each input step, the possibility of human error arises.
6. Computers make use of telecommunication lines which may be tapped. They also run on electricity and are subject to 'spikes' or electrical fluctuations which might cause loss of information.

Now, bearing these features in mind, I propose to demonstrate that there is a case for government intervention in the form of legislation, at least in so far as the consumer is concerned, using just one theme, namely, the problem of risk allocation for loss.

I have, I think, only time to discuss one theme. There have been many instances of fraud in the U.S., where many E.F.T. schemes and projects have been pioneered. Don Parker's many books and articles testify to that. Some of these frauds are not very different from the ones perpetrated in respect of paper-based transactions. For example, an employee authorised to use a particular code may initiate a transaction whereby his employer's funds are channelled into a fictitious account from which he subsequently withdraws the funds. This is really no different from the cheque situation. Other frauds are totally different. For example, those involving the tapping of telephone lines and re-directing the destination of the funds. It is true that data encryption will make it more difficult; but nothing is impossible. There is also a technique known as 'salami slicing' by which the rogue re-directs tiny slices from the total amount being transmitted (say the last few figures after the decimal point), and because he does so in this manner, avoids detection for some time. Over a period of time, especially if the funds being transferred run into the millions or billions, we are looking really at a high loss fraud. These are the big time corporate frauds. But the small, individual consumer is not immune either. His magnetic stripe card may be stolen and used to withdraw funds by a person having access to his personal identification number. You might argue that this is not different from loss arising out of the use of a forged cheque or a lost credit card, but my point is that there are crucial differences between these different payment methods.

In the case of the cheque and credit card, a signature is necessary to give validity to the transaction. In the case of a forged cheque the *Bills of Exchange Act* provides that, with certain exceptions, the signature is a nullity. There is no mandate to pay. In the case of a credit card, the signature both identifies the cardholder and authorises the transaction (at least from the cardholder's viewpoint). A signature that has been forged is an invalid authentication. This stems from the fact that a signature is personal to the person signing.

On the other hand, a personal identification number, despite its name, may not be personal. It may be known to a handful of staff at the bank, and may be used by anybody who knows what it is. The analogy of the personal identification number is therefore to be drawn not with the signature that is appended by hand, but rather with the mechanised signature which raises different issues of estoppel and negligence perhaps, but not lack of mandate.

Assuming lack of conduct which would give rise to negligence or estoppel situations, how are these losses to be apportioned between two innocent parties? In the absence of legislation and risk allocation provisions, the common law seems to provide little help. There is the dictum of Mr. Justice Ashhurst in the case of *Lickbarrow v. Mason* (1789) 2 T.R. 63, 70, where he said and I quote:

> We may lay it down as a broad principle, that whenever one of two innocent parties must suffer the acts of a third, he who has enabled such third person to occasion the loss must sustain it.

However, this principle has been criticised as being too broad and I think it would not find acceptance today. The other alternative at common law is to find liability on the part of the customer or the bank on the basis of the implied term, but this has its own difficulty. On what ground would a court be able to say that it was an implied term of the contract that the consumer should bear the loss? Or vice versa?

Connected with this problem is yet another question: on whom does the onus of proof fall? Take the example of a Handybank card which is stolen and fraudulently used to withdraw a sum of cash from an automated teller machine. Does the customer have to prove that he or she did not make that withdrawal? That is almost an impossible burden as evidenced in the American decision of *Judd v. City Bank* 435 NYS 2d 210 (Civ. Ct., Queens County, Nov. 3, 1980). There, the court had to decide whether a customer who had denied that certain withdrawals made at an A.T.M. (Automated Teller Machine), were hers was telling the truth. The bank had offered a computer printout as proof that the

withdrawals were made. Fortunately, she was able to produce a statement from her employer to the effect that she was on the job when these purported withdrawals were made. Consumers should take heart at what the court had to say:

> This court is not prepared to go so far as to rule that where a credible witness is faced with adverse testimony of a machine, he is as a matter of law faced also with an unmeetable burden of proof. It is too commonplace in our society that when faced with the choice of man or machine we readily accept the 'word' of a machine every time. This, despite the tales of computer malfunctions that we hear daily.

I am heartened to hear Mr. Douglas say that the consumer should not be placed in a position of having to prove the other party wrong, if a transaction is in dispute. But, should we leave it to the courts to arrive at this conclusion, or should we pre-empt the matter by legislation now?

Our A.T.Ms have been around for some time now and I don't know if such frauds have been perpetrated. I don't know if the banks will tell me of any. The question of burden of proof apart, there is still the next question of allocation of loss.

Let me first identify the types of losses that can arise. It is not confined to the amount being transferred from point A to B, or the amount that has been withdrawn from the A.T.M. It includes interest, exchange losses, (where, for example, company X transfers a sum of money to company Y in another country); and it includes indirect losses. Cases have frequently arisen in the English courts where the judges have had to decide whether an electronic payment was made in time, especially in relation to charterparties. A computer error of fraud could lead to the discharge of the contract. Now who is to be liable? I don't think the banks would be quite so generous as Mr. Douglas has been with the question of burden of proof.

I have with me Westpac's application form for the Handycard which has, on its back, the conditions of use of Handybank. Let me read a couple of the clauses to you. First, clause 15 provides: 'The bank shall not be liable for any loss suffered by the cardholder for the loss or destruction of any notes, cheques, vouchers or documents placed in the Handybank arising from burglary, theft, fire, explosion, earthquake, volcanic eruption or other convulsion of nature, failure of supply of electricity, invasion, act of foreign enemy, riot, revolution, civil commotion, strike, lockout, military or usurped power or martial law.' Clause 18 says, 'The Bank shall not be responsible for any loss caused by the failure of either the card or any electronic funds device or any other mechanical part of the Handybank to function properly.' You say we don't need legislation now?

In the U.S. there is a Federal Act, the *Electronic Funds Transfer Act*, enacted in 1978, which adds Title IX to the *Consumer Credit Protection Act*. It is implemented by Regulation E, which came into effect on March 30th, 1979. That has undergone a couple of amendments since but they do not detract from the basic protection conferred under that Act.

So far, I have only dealt with a few issues. The U.S. Act deals with twelve important consumer issues, namely, disclosure of the terms and conditions of transfer, periodic statements and documentation, pre-authorised transfers, error resolution procedures, consumer liability for unauthorised transfers, liability of financial institutions, issuance of cards and other means of access, system malfunctions, compulsory use of E.F.T., waiver of rights, civil liability — in that respect, measure of damages — and finally, criminal liability. I don't intend to discuss all these provisions here but would like to take you on a brief tour of the provisions in respect of the issues that I have raised.

First, the question of burden of proof. Basically, documentation generated by the system or bank constitutes *prima facie* proof of an electronic funds transfer. This applies equally to A.T.M. receipts as to periodic statements. This is to be found in Section 906. Secondly, there is a procedure for error resolution. The financial institution concerned is required to follow certain procedures where there has been either an oral or written notification of the error within sixty days after it has transmitted a document on notice alleged to

contain the error. Its responsibilities in respect of the error resolution procedures cease after the expiration of the sixty-day period. The procedures require the financial institution to investigate and report to the consumer within ten days of receipt of the error notification. Alternatively, it may provisionally re-credit the customer's account within the same period and then conclude its investigation within forty-five business days of the notice of error. Any error discovered must be rectified within one business day of discovery of the error. If there is no error it must deliver to the consumer within three business days of completing its investigations, an explanation of its findings and a notice explaining the consumer's right to documents from which the conclusions were drawn. These provisions are backed by severe penalties including the consumer's right to *treble* the amount of damages.

Regulation E contains a unique structure for determining the liability of the consumer for unauthorised withdrawals. Section 205.6 of Regulation E imposes three levels of liability. The first level comes into play where the institution is notified within two business days of learning of loss or theft of the access device. In this situation the consumer's liability is limited to the lesser of $50.00 or the amount withdrawn. Level *II* is invoked where notification by the consumer occurs between three and sixty days of learning of loss or theft. In this case the consumer is liable for any unauthorised transfers occurring within that period. Level *III* comes in where the consumer has not reported within the sixty-day period. In this situation, he incurs unlimited liability for *all* unauthorised transfers not reported within the sixty-day period.

Vis-à-vis financial institutions, the Act draws a distinction between liability for erroneous withdrawals and liability for not completing transfers. There is no liability for erroneous withdrawals and so the consumer has to fall back on the error resolution procedures for rectification of errors. But in respect of liability for not completing transfers, the institutions are liable for damage that is proximately caused by them.

It should also be noted that these provisions are not excludable.

These provisions may or may not go sufficiently far to protect the consumer. But the need for legislation, at least, in respect of consumer interests, has been recognised in the States. We may agree or disagree with the twelve areas of protection, but I think a start has to be made.

We already have a live working model, to use the words of Mr. Douglas, on which the legislation can be based. Your A.T.M. has been around for a long time. We can always amend the legislation to meet new requirements, as and when they arise.

I understand that there is a Standards Association, set up to look into E.F.T.S. to ensure, amongst other things, that message formats are uniform and to ensure that different proprietary systems may be interfaced with one another. I might remind you that a customer needs three things when verifying the status of an account. He needs a statement of account; he must examine that statement; and finally, he must complain when he discovers the error. If this association formalises the message format now, before any legislation has been enacted to protect the interests of consumers, two eventualities are possible. Either it would have to re-design a new format to meet the requirements of legislation which may require certain data elements to be input so that the periodic statements received by the consumer make adequate disclosure; or the consumer protection measures might have to be abandoned if the format cannot be changed. Of course there is a third alternative, that the Standards Association will anticipate all requirements, but that will remain to be seen.

I have, as requested by the Chairman, confined my comments to only a few issues in order to provide some depth of discussion. There are many other problems, but these will have to be discussed some other time. Thank you.