Recent Trends Affecting the Bank's Liability During Electronic Funds Transfer Operations

Thunis, Xavier

Published in:
J.I.B.L.

Publication date:
1991

Document Version
Publisher's PDF, also known as Version of record

Recent Trends Affecting the Banks' Liability during Electronic Fund Transfer Operations*

XAVIER THUNIS

Xavier Thunis, Deputy Director, Research Centre on Computer Law, Namur, Belgium

Electronic fund transfers are rather reminiscent of Bizet's Arlésienne: they are frequently spoken of, much thought about, but never seen! Lawyers have been led to ponder on this intangible reality and to ask themselves the following question: to what extent does the introduction of new information technologies (data processing, telecommunications, telematics) create new risks and new liabilities for the banker? It is this question that will be addressed very generally here, with frequent reference to existing legal sources, contracts, case law and occasionally to legal directives or draft legal directives.

Definition and Concept

What must be stressed first of all is the rather imprecise and badly defined nature of the expression 'electronic fund transfer' (EFT), which makes its own contribution to the air of mystery which surrounds the subject. In current parlance, the expression is generally used to describe withdrawal services from automated bank teller machines and payments services via a point of sale terminal or a home terminal. But this is only part of the story. There is another aspect which the user of payment instruments does not see – the invisible part of a payment operation. This is the relationship between the banks which has been given over to advanced automation by the major players in the league.

The phenomenon, therefore, affects both relations between the banks and the bank/client relationship. This leads to the initial problem of developing a *global* approach towards the effects of automation, starting with the issuing of the order by a transferor, via its transmission to the interbank exchange networks, right through to final payment of the transferee by crediting his account.

The second problem is that automation can be more or less advanced depending on the type of relations envisaged, and can give rise to what is sometimes known as 'semi-electronic movements of funds'. Thus, in the case of cheque truncation, there is also a document which is written and signed by the customer when the order is issued, namely the cheque. However, the cheque is no longer physically transmitted between banks. The banks exchange certain data (amount, name of the drawer, and so on) relating to the cheque, without actually moving the cheque. This excludes the possibility of certain traditional safety procedures, such as checking the signature. It will, therefore, be necessary to reconcile the somewhat stringent rules governing the issuing and circulation of cheques with rules instituting new control and exchange procedures at the inter-bank level.

The third problem is that automation is a polymorphous phenomenon: magnetic tapes, diskettes, remote transmission from a terminal, cards with magnetic strips or microchips are all methods used to transfer funds. This technical diversity makes a global approach to the phenomenon difficult since the lawyer finds himself lost in a maze of technical minutiae and loses sight of the fundamental legal questions, particularly those of proof and liability.

This problem is particularly noticeable in the rare attempts which have been made to legislate on the subject. A wide range of criteria have been used. Thus, § 903(6) of the Electronic Fund Transfer Act (EFTA), the American federal regulation which came into effect on 10 May 1980, states that '. . . the term "electronic fund transfer" means any transfer of funds, *other than a transaction originated by check, draft or similar paper instrument*. . . .' The criterion adopted is the disappearance of the paper medium. However, American law takes account only of the issuing of the order, which must be carried out by a *consumer*, and ignores interbank relations, which are regulated, in particular, by the new Article 4A of the Uniform Commercial Code (UCC) which applies to 'wholesale transfers'. Similarly, the recent European recommendations of 8 December 1987 and 17 November 1988[1] concentrate on a particular instrument – payment by card.

The following basic established fact may be taken as a starting point: the *account* plays a central role in the electronic fund transfer operation. Electronic fund transfers are never any more than the automated exchange of messages from the client to the bank, between different banks and then from the bank to the transferee. This exchange of messages finally results in a set of written messages to debit or credit the respective accounts. No 'funds' are

* This paper is a slightly revised version of a paper given at the International Chamber of Commerce on 24 April 1991.

1. OJEC 24 December 1987, L365/72 and OJEC 14 November 1988, L317/55.

exchanged as such, the procedure simply involves variations in the debits and credits to the accounts concerned, which can be carried out more quickly due to the use of automated techniques. In law, the basic effect of these automated techniques is a *dematerialisation* of the operations, that is to say the total or partial disappearance of the written paper which is signed at the time of issuing, transmission or execution of payment orders.

Electronic fund transfers may therefore be defined as the set of payment techniques which have the effect, on the one hand, of totally or partially eliminating the use of paper documents bearing a written signature for issuing or executing payment orders and, on the other hand, of replacing these paper documents by electronic pulses which can be processed directly by computer.[2]

This is an extremely broad definition which enables the legal problems raised by EFTs to be studied between the various actors involved:

- between banks;
- between banks and their customers, whether these customers are companies (corporate banking) or private individuals (retail banking).

Legal Sources

There are three types of source corresponding to three possible approaches to the phenomenon.

Contractual approach

A whole series of contracts exists between banks and their customers. These contracts regulate the legal problems resulting from the use of automated techniques. These are notably contracts drawn up with *consumers* who use their cards at point of sale terminals (POST) or automated teller machines (ATM). It also includes contracts drawn up with *companies* using magnetic tapes for transmitting orders and the so-called homebanking contracts which are also drawn up with companies which want to issue transfer orders from terminals on their premises.

Despite their diversity, all these contracts govern the same type of problem. They determine in particular:

- the conditions for accessing the service;
- the obligations of the holder of the means of access (vigilance and confidentiality in protecting the means of access);
- the liabilities of the parties in case of loss or theft;
- the proof of the operations carried out (since the written signature disappears, the permissible elements of proof and conclusive evidence associated with it must be determined).

Associative approach

As the use of electronic methods for processing and transmitting orders becomes more widespread, associative structures emerge. This is the case of those groups which carry messages at the national level, such as Banksys in Belgium, or internationally, such as SWIFT. This is also applied to the national clearing houses, the CEC in Belgium (Centre for the Exchange of Clearing Operations), SAGITTAIRE in France, or CHIPS in the United States.

Although sometimes tightly controlled by the public authorities, all these groups have their own rules to regulate the standards to be upheld by their members and their liabilities where problems occur with payments. This is particularly striking in the case of SWIFT which, very precisely, delimits, in its statutes and other 'policy volumes', both its own obligations and those of the sending and receiving financial institutions.

Legislative and paralegislative approach

Even though EFTs are a relatively new phenomenon, they have already given rise to a number of legislative initiatives which will not be examined in detail or even listed here. The laws of the United States, Denmark and France governing the use of cards are known. It is interesting to note that the international and technical nature of the subject appears to assign certain limits to national law: so there have emerged regulatory principles (CCI), a particularly notable Legal Guide relating to ETFs (UNCITRAL) and a European code of good conduct relating to payment by card (see above). This is, perhaps, a classic phenomenon, although the behaviour of the national or European public authorities is less traditional as they themselves adopt the technique of codes of good behaviour or guidelines. We can thus see the birth of 'soft' or mitigated forms of public intervention.

The Banker's Liability in Relation to ETF – Problems with Payment

A wide range of risks or incidents relating to payment are possible. They can be classified into three categories.

2. This definition is inspired by that proposed by M. Vasseur in 'Le paiement électronique – aspects juridiques' (Electronic payment – legal aspects), JCP, 1985, 1, 3205 no. 7.

(1) In the first set of hypotheses, there is no order from the authorised transferor. This may be attributable to an error by the financial institution, usually the result of fraud, whereby a third party uses the means of access of a legitimate title holder in order to make a transfer.
(2) In the second set of hypotheses the order is correctly issued by the authorised transferor, but the transfer proves to be irregular, either in terms of the amount or identity of the transferee. This can either be due to error or fraud.
(3) The genuine order is correct in all aspects and remains correct, but it is not carried out by the bank or execution is delayed due to, for example, a failure or interruption of the data processing system.

This outlines in very rough terms the main risks inherent in the issuing and execution of transfer orders. The realisation of these risks can occasionally give rise to considerable damages: loss of all or part of the principal amount, loss of interests and even loss of a contract due to the imposition of penalty clauses because the order has not been preformed correctly (see *Evra Corp.* below).

Overview of the Banker's Liability in Relation to ETF

Several hypotheses of the banker's (or bankers') liability in relation to ETF may now be examined, distinguishing between the type of relationships involved (relationship between the bank and the transferor – company or consumer) first of all, and then interbank relations.

Relationship between bank and transferor

The transferor is a company

Contractual provisions
A company wants to issue orders using automated means by linking its own data processing system with that of the financial institution.

Contracts with names such as 'Electronic banking', 'Financial telematics' comprise a whole range of stipulations relating to implementation of the service, the means of access to the service, the availability of the system, the security standards to be upheld both by the customer and by the financial institution in relation to the holding and periodic renewal of access codes. Two types of clause are examined below.

Clauses relating to the unforeseen occurrence of an outside cause. A traditional first clause establishes that

> the bank undertakes to perform its services with all due care and diligence. However, the bank is not liable for any errors or anomalies arising from breakdowns or other failures of the public data transmission networks.

This does not deviate significantly from common law.

A second type of clause considerably broadens the concept of *force majeure* by indicating, for example, that

> the bank may under no circumstances be held liable for a temporary interruption of the service due to events beyond its control, such as a breakdown, the telephone lines being cut off, strikes or circumstances justifying such an interruption, particularly for work leading to improvement of the existing equipment. The bank shall, however, take all measures in its power to limit such interruptions to a minimum.

As such, strikes do not automatically constitute a case of *force majeure*, but the parties can stipulate that any strike will be considered as an exculpatory factor. As far as breakdowns are concerned, the problem is to decide what type of breakdown is involved – power cut; fire; computer failure or software bug which blocks an entire processing system.

The inclusion of this last case unquestionably broadens the concept of *force majeure*. In the author's opinion, the bank should, in principle, have access to back-up equipment which is sufficient to permit the system to continue to operate (see below).

A third type of clause is conceivable here, whereby the transferring bank is exempt from any liability for delays or losses caused by the intermediary banks, clearing houses, interbank carriers (such as SWIFT) and, more generally, by the services of a third party. This type of clause is rarely found in 'Electronic Banking' contracts, but is frequently found in general regulations governing operations.

Such a clause, although clearly understandable from the viewpoint of the transferring bank, creates difficulties from a legal standpoint. On the one hand, it is normal for a bank not to want to be held liable for the faults of a third party. In certain cases, the bank has no real choice of third party: recourse to clearing houses may be imposed by the law or the transferor himself may have required a transfer via the SWIFT network. In other cases, the choice is reasonable: a well-known and trusted bank chosen as the correspondent bank goes bankrupt, which could not have been foreseen. On the other hand, the transferor, by virtue of such a clause, is deprived of any right of action against his own bank and does not, in principle, have direct contractual recourse against the correspondent bank (unless it is considered that the transferor benefits from some sort of stipulation covering other parties involved in the agreement between the banks – but this is very uncertain). As for action on a delictual basis (based

on Article 1382 of the Civil Code), this is uncertain and questionable from a theoretical viewpoint.

This situation may not find a satisfactory solution within the framework of the traditional rules on liability. Even if the transferor's bank has not been negligent in its choice of third party, is it fair to impose the risk of the operation on the transferor? For this reason, some writers advocate that the risks be imposed on the transferor's bank, referring to the field of transportation of goods which is governed by the CMR convention. This stipulates that 'the carrier shall be responsible . . . for the acts and omissions of its agents and of any other persons whose services he might use for performance of the carriage'. This is a significant precedent which could inspire possible guidelines relating to electronic fund transfers.

Clauses relating to unauthorised transfers: proof of operations. The following clause illustrates the way in which contracts deal with the consequences of possible fraud:

> The direct or indirect consequences which might result from the misuse of the service, either by authorised users or by third parties, shall not be borne by the bank. The subscriber hereby agrees to assume full responsibility for such misuse.

The customer is responsible for the fraudulent actions of his employees (authorised or not) and those of third parties. His account may, therefore, be debited in the amount of any transfers carried out even if they are forged. The justification for liability resting with the customer could be found in the traditional concept of fault, although the concept of risk appears a more appropriate basis. This type of solution is understandable because the customer controls – or should control – the locations from which the order is issued.

It should also be noted that the customer's liability can also be extended to cover the transmission of the message between his computer system and that of the bank through the use of clauses governing *evidentiary* problems.

Thus, contracts painstakingly provide for the onus of proof by stipulating, for example, that

> the log (computer generated list of transactions carried out) produced by the bank constitutes formal and satisfactory proof of the orders issued by the subscriber.

The system operates as follows. The log generated by the bank's computer is deemed to register the customer's instructions faithfully. This means that the customer is liable for the order issued from his premises until it reaches the bank's computer. He is, therefore, liable for any acts of fraud committed over the telecommunications lines between his premises and the bank. All this shows that there is a close connection between questions of proof and of liability.

The transaction must not be of an obviously unusual nature, in which case, it should attract the attention of the bank. A transaction may be of an obviously unusual nature if, for example, the amounts are higher than normal or if the transaction is addressed to a recipient not previously known to the bank. However, the problem with electronic fund transfers is that checks based on a personal element of the transferor tend to disappear, and assessment is reliant on the quality of the system implemented.

If the fraud has been facilitated by an inadequate security system implemented by the bank, it appears that the bank's liability is brought into play. Although it is true that the customer (a company and, therefore, a professional) chooses his means of payment, the banker (as a professional credit organisation) should be held primarily responsible for the data processing system he offers for organising and rationalising his banking services.

In the United States, twelve states have adopted a new Article 4A relating to electronic fund transfers. This new Article, which covers wholesale wire transfers, stipulates, in particular, that

> A payment order received by the receiving bank is effective as the order of the customer, whether or not authorized if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders. . . . Commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, including the size, type and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated.[3]

The principle involves imposing the burden of implementing reasonable security arrangements on the bank. These must be capable of preventing frauds because the bank is in the best position to implement such arrangements. A similar approach has been adopted by the UNCITRAL working party.[4]

Jurisprudence: delays in the execution of the order (Evra Corp. v Swiss Bank Corp).[5] A detailed discussion of the facts is useful at this point. In 1972, Hyman Michaels Company, a Chicago-based scrap metal dealer (which became Evra Corp. in 1976) entered into a two-year supply contract with a Brazilian company. Hyman Michaels chartered a ship, the *Pandora*, to carry the scrap. Under the terms of the charter, monthly payment for the hire of

3. Article 4A 202(b) and (c).
4. A/CN9/W6 IV/WP 39 page 12 onward.
5. 673 F.2d 951.

the ship was to be made two weeks in advance and, if not made on time, the *Pandora*'s owner could terminate the contract. Payment was to be made by bank transfer to the owner's account at the Banque de Paris et des Pays-Bas in Geneva.

The usual method used by Hyman Michaels was to request the Continental Bank of Chicago, where the company had its account, to make a wire transfer of funds to the shipowner's Swiss bank account. The procedure was as follows. Continental would debit Hyman Michaels' account by the amount of the payment and would then send a telex to its London office for retransmission to Swiss Bank, its correspondent bank in Geneva, asking Swiss Bank to deposit the amount in the Banque de Paris account of the ship's owner. In turn, Swiss Bank's account at Continental would be credited by the same amount. When Hyman Michaels chartered the *Pandora* in June 1972, the market was in its favour, but the charter rates began to climb and the ship's owner made several attempts to terminate the contract for reasons of late payment. On the morning of 25 April 1973, Hyman Michaels telephoned Continental and asked for $27,000 to be transferred to the *Pandora*'s owner at the Banque de Paris in payment for the charter hire period from 27 April to 11 May 1973.

Since the charter contract stipulated payment in advance, payment had to be carried out before the close of business on 26 April. Continental sent a telex to their London office on 25 April, which reached England during the night. Early the next morning, the telex operator in London made several unsuccessful attempts to contact Swiss Bank. The operator then tried another Swiss Bank number in the foreign exchange department. This machine acknowledged receipt of the message. However, the Swiss bank did not act on the payment order and no transfer was made to the shipowner's Banque de Paris account. Nobody knows exactly what went wrong, although there was some speculation that the receiving telex machine had run out of paper such that the message was never printed. On the morning of 27 April, Hyman Michaels was notified by telex that the charter contract had been terminated for reasons of non-payment.

Days passed while the banks unsuccessfully searched for the lost telex message, and finally Swiss Bank suggested that Continental should retransmit the message. This was done on 1 May. The next day (2 May), Swiss Bank attempted to deposit the money in the shipowner's Banque de Paris account, but the payment was refused. A panel of arbitrators concluded that the shipowner was entitled to terminate the agreement because Hyman Michaels, although blameless until the morning of 27 April, had not done everything in its power to remedy the situation. The arbitrators held that Hyman Michaels should have immediately issued a duplicate order, rather than relying on the banks to resolve the problem.

Hyman Michaels then brought an action against Swiss Bank in order to recover both its expenses in the arbitration procedure and the loss of profits resulting from termination of the highly advantageous contract. (After termination of the contract, Hyman Michaels had to pay a charter hire fee double that of the previous rate.) In the end, due to cross claim and counter claim procedure, all the banks were involved in the case.

The case was tried by a district judge without a jury.[6] The judge held that the case was governed by the law of the State of Illinois, and that, under it, Swiss Bank had been negligent. This negligence had resulted in the loss suffered by Hyman Michaels. Swiss Bank was, therefore, liable to Hyman Michaels for $2.1 million in damages ($15,000 for arbitration costs and the rest in lost profits). Neither Hyman Michaels nor Continental were held to be negligent. The Court of Appeal reversed the decision, holding that Swiss Bank could not be held liable for consequential damages, even though it had been negligent, because it had not been notified of any special circumstances linked to the transaction under consideration.

This decision provides a good illustration of the typical problems encountered in the context of electronic funds transfers.

The choice of applicable law when the parties to litigation are of different nationalities. This will not be discussed in detail here, although the importance of the issue should be emphasised.

Under Swiss law, the bank cannot be held liable to someone with whom it is not in privity of contract, and there was no contract between Swiss Bank and Hyman Michaels. In contrast, Illinois State law does not have such a privity requirement.

However, without much justification, the Court of Appeal held that this issue did not have much effect on the final outcome.[7]

The type of damages covered. Several types of damages are applicable when an electronic funds transfer is delayed by the bank:

- Capital loss, loss of interests or the fee paid for the transfer. Under American law these are direct or 'general' damages. Hyman Michaels was not seeking indemnification for direct damages, since the amount transferred was not lost. The debited account did not bear interest and Hyman Michaels paid no fee for the failed transfer.
- Consequential or special damages. These are caused by failure or a delay in carrying out a contractual undertaking (payment of sums of money) leading to imposition of a penalty clause or termination of a highly profitable contract.

6. 522 F. Supp. 820 ND Ill, 1981.
7. See page 955.

The law applied by the Court of Appeal in the *Evra* case stipulates that only general damages are taken into account and give rise to indemnification unless, at the time the request for transfer of funds is made, the bank is notified of the type of transaction and the consequences of delayed transfer.

Swiss Bank was not, therefore, held liable for the consequences of its gross negligence (failure to respond to the telex message), although this uncontestable negligence was the root cause of Hyman Michaels' loss.

Could the sole use of the electronic funds transfer system be considered as sufficient to make Swiss Bank aware of the situation? The responses to this question varied. The first judge held that

> the fact that the plaintiff was transferring funds by wire rather than through the mail was sufficient to alert Swiss Bank to the importance of the transaction.[8]

Conversely, the Court of Appeal held that

> Electronic fund transfers are not so unusual as to automatically place a bank on notice of extraordinary consequence if such a transfer goes awry. Swiss Bank did not have enough information to infer that if it lost a $27,000 payment order, it would face a liability in excess of $2 millions.[9]

Swiss Bank was not given sufficient information to know that it was assuming a liability in excess of $2 million if it lost a $27,000 payment order.

In its decision, the Court of Appeal appears to have taken account of the absence of a contract between Hyman Michaels and Swiss Bank:

> Privity is not a wholly artificial concept. It is one thing to imply a duty to one with whom one has a contract and another to imply it to the entire world.[10]

However, was Swiss Bank really a third party since, as the court acknowledged,

> it knew or should have known, from Continental Bank's previous telexes, that Hyman Michaels was paying the Pandora Shipping Company for the hire of a motor vessel named Pandora.[11]

It can be seen, therefore, that in order to receive compensation, a damage must be foreseeable. This is the basic principle under French law.[12] The same is true under Anglo-Saxon law, whereby compensation may only be paid for general damages. However, the problem here is to determine in fact what is foreseeable and the criteria on which this decision should be based. Should not the transfer method used and the 'quasi' contractual relationship between the customer and the correspondent bank be taken into account when assessing foreseeability?

In the opinion of the banks, the decision does not provide a realistic solution to the problem of bank liability for consequential damages (what information would be required for adequate notice? Is it really practicable to send notice for thousands of messages each day?).

What kind of diligence can reasonably be expected from the customer and from the banks? Assessment of fault. If the traditional criterion of fault is applied, there is no doubt that Swiss Bank committed an act of gross negligence by failing to provide a system for checking the telex machines. Furthermore, the telex machines were operated by inexperienced employees. The first judge held that 'such a cavalier attitude towards major transactions by a sophisticated international bank [is] shocking'.[13] The Court of Appeal also noted Swiss Bank's negligence, but this was not taken into account for allocation of damages, since these were not predictable.

Continental was also criticised for not having notified Swiss Bank that significant sums of money were involved. Neither bank took adequate action when it was discovered that payment had not been made, thus wasting five or six days in tracing the lost instruction.

In brief, the Court of Appeal insisted on Hyman Michaels' negligence, holding that it was imprudent in waiting until the last possible moment before instructing its bank to make the transfer. In the opinion of the Court,

> the action taken was immediate but did not prove to be adequate in that [Continental] Bank required some 5/6 days to trace and effect the lost instruction to remit. [Hyman Michaels] could have ordered an immediate payment – or even sent – a banker's check by hand or special messengers, so that the funds could have reached owner's bank, not later than April 28th.[14]

This last passage is very clear: although recognising the banks' lack of efficiency, it holds the customer responsible for a routine wire transfer and for choosing the best way to effect payment instead of the two banks. The consequence is the following. Continental Bank, which was aware of the circumstances surrounding the transaction, was not held liable because non-execution of the payment was caused by a negligent act by Swiss Bank. However, Swiss Bank, which had been manifestly negligent, was not held liable because it had not been notified of the exceptional circumstances of the transmission. Consequently, the customer remained liable for the loss.

Such a result appears unacceptable. Electronic techniques increase the speed with which transfers of funds can be made. It is clear that a higher degree of diligence on the part of the parties involved is

8. 522 F. Supp. 820 (1981) page 833.
9. 673 Fed 951 page 956.
10. *Ibid.*, at page 956.
11. *Ibid.*, at page 958.
12. Civil Code, Article 1150 onward.
13. *Ibid.*, at page 829.
14. *Ibid.*, at page 954.

required. Indeed, the customer has to react promptly when he identifies an anomaly, either by reading the statements of account sent to him by the bank on a regular basis or by notice from his contracting party. However, given the use of electronic techniques, customers' expectations of prompt, reliable and effective service will also be seen as increasingly legitimate.

Here, the total lack of adequate security systems must be considered as gross negligence, or as a fault (Article 1382 of the Civil Code).

In the *Evra* case, both banks were seen to have been negligent. The correct solution should have been to hold both banks jointly liable (*responsabilité in solidum*) to the customer and to force them to settle the problem of damages between themselves.

However, it should be noted that case law subsequent to *Evra* has not been established in this way. As far as the author is aware, all the decisions taken since then confirm that the bank cannot be held liable for consequential damages resulting from delayed execution of an order.[15]

The transferor is a consumer or a particular user acting in his own interests

Electronic funds transfers by the 'general public' also have significant effects on the possible development of bankers' liability for payment.

Here again, contractual stipulations and applications of case law add new features to the banker's liability. Two Belgian case law decisions may be considered by way of example which, in the author's opinion, can be used to provide general information because they answer a wholly general question: what are the banker's obligations when the customer notifies him of loss or theft of his means of access (his card and, where applicable, the PIN number)? In other words, what is the banker's liability in the case of *stopped payment* – notice of prohibition of payment given by the card holder?

The banker's liability if payment is not stopped

In Belgium, contracts drawn up between the bank and customer has orders issued from terminals located in public places are based on the following system. The account holder bears the entire risk of any transactions carried out following the theft, loss or misuse of the means of access, up to the time at which he notifies the bank of illegal transactions or the risk of illegal transaction and up to the time the bank is able to take adequate measures to prevent any further transactions. The stipulations relating to the administration of proof confirm the account holder's liability, which ceases at the moment he notifies his bank or when the bank is able to take the normal measures to avoid commencement or continuation of any financial loss which might result from the fraudulent use of the means of access.

In global terms, this system is common to three 'regulations' governing the use of payment cards in Belgium (Mister Cash, Bancontact, Postomat).

This system is recommended in Articles 8.3 and 8.4 of the European Guideline of 17 November 1988, with the important proviso that the account holder's liability, before notification, is *limited* to ECU 150.

In brief, notification switches the burden of risk. Before notification, misuse can be due only to negligence or oversight on the part of the account holder. Once notification has been sent and after a reasonable period for the bank to act, it is negligence on the part of the bank (or the company providing the services) which gives rise to any subsequent damages, by not implementing adequate security standards.

This system must be borne in mind in order to understand the decisions of the Liège Commercial Court on 19 January 1984 and the Liège Court of Appeal on 2 February 1985.[16]

The problem relates to fraudulent withdrawals after the loss of a card, namely withdrawals subsequent to notification of the loss by the account holder. The judges had to decide who (the bank or the customer) should bear the loss of the amounts withdrawn (B.Fr. 73,000) between 1 March 1982, when the customer notified the bank that his card was lost, and 19 April 1982, when, following complaints from the customer, the bank actually took the necessary measures to make the lost card unusable. As always, there is no easy answer since both the customer and the financial institution had, in effect, failed to fulfil their obligations.

According to the Commercial Court, the customer, contrary to the regulation, had committed a fault by letting his son know his secret code, and had been negligent in not checking his account statements between 1 March and 16 April (the date on which he identified the fraudulent withdrawals). On the other hand, the bank had not taken the necessary measures to prevent use of the card after its disappearance had been notified to the bank.

Faults had, therefore, been committed by both parties. Could this justify liability being shared between both parties? Clearly, both the Commercial Court and the Court of Appeal rejected this solution and held that the bank had sole liability.

For obvious reasons, the following justification was given:

> whereas . . . Article 5 of the 'Bancontact' regulation imposes an obligation of result on the banker, any

15. See, for example, *Central Coordinates Inc. v Morgan Guaranty Trust Co.* recorded in the International Financial Law Review, July 1985, at page 37. For further details see S. Karageorgiou, *Electronic Funds Transfers: Technical & Legal Overview*, thesis, London 1990, at page 273 onward.

16. For the decisions and commentary, see B. Amory and X. Thunis, note under Trib. comm. Liège 1984 *Dr. Inform.* 1984/2, at page 29; B. Amory, note under Liège 22 February 1985 *Dr. Inform.* 1985/3, at page 28.

> failure on his part shall constitute the *exclusive cause* [*emphasis supplied*] of the withdrawals carried out after the bank had the opportunity to take the necessary steps to prevent such withdrawals.[17]

In brief, the bank has sole liability for fraudulent withdrawals after notification, even if the customer has previously committed the fault of revealing his secret code to a third party.

The banker's liability in relation to the security of the system

Two decisions unpublished for many years were handed down by the Verviers[18] courts in a particularly interesting case. On Sunday 31 October 1982, a Postomat card holder had a bag stolen from her car. This bag contained both her card and a diary listing her PIN number. The victim wanted to notify the Post Office as soon as she became aware of the loss, but was unable to do so until 2 November, when the counters opened, since the system for notification of lost or stolen cards did not operate at night, during weekends or on public holidays. The industrious thief took the opportunity to debit B.Fr. 40,000 from the account during the intervening period.

While admitting the fault of the holder of the means of access, the Verviers jurisdiction held that the loss should be borne fully by the Post Office, because its system did not offer adequate security, and thus constituted the direct cause of the damages. The reasons adduced by the conciliation magistrate are particularly clear in this respect:

> Whereas with good reason the plaintiff asserts that by implementing a system which is completely unusable at the security level at weekends, while it is at precisely this time that the system is most likely to be used, particularly by thieves, without clearly and precisely notifying users of this fact, the defendant has committed a fault . . .
>
> Whereas the fault committed by the defendant renders ineffective the fault previously committed by the plaintiff. . . .

Faced with this delicate problem of attributing illegal debits made possible by the simultaneous fault of both customer and financial organisation, the Verviers courts decided along the same lines as the Liège courts: once the customer has stopped payment, no further causal link exists between a fault committed by him and debits subsequent to stopping payment, for which the bank is exclusively responsible. This raises the basic question of what exactly is the effect of notification. However, the case before the Verviers courts had a different purpose. The aim was to decide who is responsible for the provision of services and the level of security which the consumer is entitled to expect (see below).

Interim conclusion

Without reviewing all the case law relating to incorrect or falsified orders resulting from EFTs carried out on behalf of the general public, it can be said that two major factors determine the banker's liability: a legal factor and a technical factor.

(1) *Legal factor*. Given the disappearance of the personal elements (such as signature and so on) which can be used to authenticate the transfer order, the financial institutions take care to specify that data records constitute an admissible or even restricting element of proof if the origin, amount or recipient of the order is disputed. Thus, the following clause:

> The customer accepts without reservation that orders are transmitted and carried out in accordance with the data recorded by the Bank. He acknowledges that the data recorded by the Bank is consistent, correct, precise and restricting for all parties.

This is clearly designed to render the customer responsible for fraudulent orders transmitted using his means of access. Such clauses relating to proof are valid in principle and they are more likely to be taken into account by the judge if the transfer system is reliable (see below).

(2) *Technical factor*. Reliability of the systems implemented. The level of security of these systems will clearly influence the judge's assessment, and therefore the banker's liability.

There is a trend to impose on the banker the obligation to offer an EFT system whereby, as discussed earlier, the level of security is reasonable in the light of technical developments, the risks of fraud and the state of the market. Recent papers have explicitly stipulated this obligation, such as recommendation 10(1) of the Jack Report, which indicates that

> Banks should therefore adopt the principle that an EFT system must meet certain minimum standards in its authorization procedures, so as to provide an acceptable degree of protection for the customer against the consequences of unauthorized instructions.

It is also in the banker's interest to look after his security system for several reasons.

> (1) Since he can no longer directly check the authenticity of the order, a reliable system is the only guarantee which will ensure, with maximum probability, that the person issuing the order is indeed the authorised transferor.
> (2) If the system is reliable, that is to say if transmission of a fraudulent order is not due to failure of the security system, but rather to a negligent act by the customer who has not observed the security instructions (such as not

17. For information, Article 5 of the Bancontact regulation indicates, in particular, that if the card is lost or stolen, 'the financial institution shall take the necessary steps to prevent fraudulent use of the card'.

18. J.P. Verviers 29 November 1984 et civ. Verviers 8 January 1986 D.I.T. 1988/3 at page 58 onward, note M. Schauss.

disclosing the PIN number to a third party). This is the solution currently adopted by the French and Belgian Commercial Courts, which require the user to prove a malfunction of the system, which is not an easy task.

(3) If the system is reliable, that is to say if the operating and media storage conditions are correct, in disputed cases, the judge will rely on the data records produced by the bank and will assume that the order, even if it is fraudulent, must effectively be imputed to the holder of the means of access.

(4) The system *must* be sufficiently safe to be able to quickly and effectively stop payment when notification is received from the user, since, more and more, case law and legal stipulations (EFTA, Danish law relating to cards, European guideline, and so on) consider that once notification to stop payment has been received, the holder of the means of access is definitively released from liability.

Interbank relations

The problems of liability are no less delicate in the case of interbank relations. What are the obligations of the various bankers in terms of vigilance and diligence? These complex problems must take account of the development of relations between the partners in the transfer, which will decide whether they are part of an electronic message transfer (SWIFT) or electronic funds transfer (CHIPS) network.

Between banks operating outside an interbank network

The most 'straightforward' case is where two banks are involved in the transfer, both of which accuse the other of lack of vigilance or diligence. American case law provides several interesting examples of this type of litigation.

Obligation of diligence

The first example does not involve electronic fund transfers in the true sense of the word, but rather the obligation of diligence which applies between banks with computerised cheque processing systems. It is relevant, however, because it gives rise to the following question: to what extent does failure of a data processing system constitute a case of *force majeure*?

In the United States, the 'midnight deadline' rule applies between the drawee bank and the depositary bank. This is the period during which the drawee bank must return an unhonoured cheque, after which it will be held definitively liable for payment of the cheque.

However, the American commercial code stipulates a number of circumstances which release the drawee bank from the consequences of a delay in returning the cheque:

> interruption of communication facilities . . . war, emergency conditions or other circumstances beyond the control of the bank provided it exercises such diligence as the circumstances require.[19]

Can the drawee bank use the excuse of a failure in its data processing system in order to discharge itself from the consequences of a delay in returning an unpaid cheque? American case law appears to have developed somewhat in the response it gives to this question.

In *Port City State Bank v American National Bank*,[20] a memory error in the American National Bank's data processing system made it totally inoperative, just after it was installed. The consequence was that several cheques were returned after the stipulated deadline. The court held that the event was beyond the drawee bank's control and that the bank had shown sufficient diligence in immediately calling in the system supplier who guaranteed rapid rectification of the situation. The court also held that American National Bank could not be criticised for not reverting to a manual processing procedure, because this was no longer in operation at the bank. As soon as it became clear that the repair would take longer than expected, American National Bank engaged the back-up services of another bank.[21] There were, therefore, reasonable grounds for exercising the exculpation stipulated in the Code, given the circumstances and the steps taken to limit the extent of the damage.

However, as data processing systems become more widespread, and are starting to reveal their secrets and inadequacies, the assessments of the American courts are becoming increasingly severe.

Thus, in *Blake v Woodford Bank & Trust Co.*[22] the court held that the large number of cheques to be processed over the Christmas period, combined with an interruption in the operation of the automatic posting machine, was not an unforeseeable event[23] which could release the drawee bank from its obligation to observe the midnight deadline. It appears that the American courts no longer automatically consider failures in a data processing system to be necessarily unforeseeable (acts of God) and that they now examine the actual circumstances behind the incident. In particular, they emphasise the need for back-up procedures and contingency plans which enable incidents to be foreseen or at least limit their effects.

The bank's obligation to ensure that its system is secure also comprises the obligation to implement a

19. UCC section 4-108.
20. 486 F.2d 196 (10th Cir. 1973).
21. *Ibid.*, at page 198.
22. Ky App., 555 S.W. 2d 589.
23. *Ibid.*, at pages 595 to 597; for another case, see *Bank Leumi Trust Co.*, 499 F. Supp. 102 (1980).

certain number of contingency plans which will ensure *continuity* of the service, *even if the data processing system fails*. This is important and clearly illustrated by the wide range of back-up procedures and contingency plans made by the large networks, such as SWIFT or CHIPS.

Obligation of vigilance

The second set of examples, again drawn from American case law, involves credit orders sent electronically between banks. The problem starts when a fraudulent transfer order is issued by a bogus transferor. The transfer order is then transmitted electronically between the banks. The fraud is successful when the depositary bank credits the indicated account number without noting the discrepancy between the number and name of the transferee. Which bank is responsible: the sending bank (because it did not detect the fraud affecting the transfer order) or the receiving bank (because it did not check that the transferee's account name and number both tallied)? American case law does not give a standard answer to this delicate problem.[24]

In the case of *Securities Fund Services v American National Bank and Trust Company of Chicago*,[25] the sending bank was defrauded by persons who, by forging the signature of a Mr Bushman, transferred $2,017,857.50 to the account of 'John Bushman Trustee // 204471'. The receiving bank credited the account number in question without noting that Mr Bushman did not have an account with them. The perpetrators of the fraud withdrew the funds and disappeared with the money. The sending bank reimbursed Mr Bushman and took action against the receiving bank.

The court upheld the plea and considered that the receiving bank, as the sending bank's 'agent', had a duty of reasonable care towards their client.[26] The receiving bank had an obligation to detect the discrepancy between the name and number of the account and was responsible to the sending bank for the damages resulting from its failure to do so, namely the lost funds.[27]

The facts of *Bradford Trust Co. v Texas American Bank Houston*[28] are worth describing in greater detail because they provide a concrete example of the ingenuity of certain criminals and the possible effects on the banks' control systems. Two 'artistes' (*sic*) arranged to buy some rare items and other valuable objects from Colonial Coins, a Houston-based company. The transaction amounted to some $800,000, which the two perpetrators of the fraud undertook to pay by transferring the funds from 'their' account held at Bradford Trust (the sending bank) to Colonial Coins' account at Texas American Bank in Houston (which later became Southern Bank – the receiving bank). A forged message was sent to Bradford Trust, asking them to buy for $800,000 some shares belonging to a Mr F. Rochefort and to transfer the funds to F. Rochefort's account, no. 057-141. In fact, the account number in question was Colonial's. Since Mr Rochefort did not have an account at Texas American Bank, Bradford Trust ordered its correspondent bank (State Street Bank) to make the transfer, which was done via Fedwire.

On receiving the funds, the receiving bank (Texas American Bank) informed Colonial that its account had been credited. Colonial then delivered the valuables to the perpetrators of the fraud who disappeared without trace. The fraud was discovered when the real F. Rochefort, who had been informed of the withdrawal by Bradford, indicated that it had not been authorised by him. Bradford recredited F. Rochefort's account and took action against the receiving bank in order to recover the funds.

Initially, the court divided the loss between the sending and receiving banks, judging that both had been negligent. The Court of Appeal overturned the decision. While acknowledging that the receiving bank had been negligent in not noting the discrepancy, the court held that the sending bank should bear the damages in full. Since it had had most dealings with the perpetrators of the fraud, it was also in the best position to avoid the loss.[29]

The solution in the Bradford Trust case involved releasing the receiving bank from its obligation to verify the agreement between the transferee's name and the account number in the order. This decision has been both criticised[30] and approved[31] (see below).

The *Legal Guide of the UNCITRAL* explicitly envisages the hypothesis whereby the receiving bank receives an order containing a discrepancy

24. Simply the main trends will be outlined here. For detailed discussion of the applicable American case law, see E. Patrikis 'Developments in the Law of Large-Dollar Electronic Payments in the United States', R.D.A.I. 7/1987, R. Effros, 'A Primer on Electronic Fund Transfers' in *The Law of International Trade Finance*, Norbert Horn (ed.), Kluwer 1989, at pages 176 onward; H.S. Koh, 'Liability for Lost or Stolen Funds in Cases of Name and Number Discrepancies in Wire Transfers: Analysis of the Approaches Taken in the United States and Internationally', *22 Cornell Int'l Law Journal* 1989, at page 98 onward.

25. 542 F. Supp. 323 (N.D. Ill 1982).

26. *Ibid.*, at page 327.

27. For an overview of the various theories on which the court based its decision see R. Effros, *Op. cit.*, at page 177, where he comments on another similar case (*Shearson/American Express v American National Bank* (Slip. Op. N° 83-C-0555, 18 August 1983). It appeared that Shearson had asked Chemical Bank to wire $1 million to American National Bank in Chicago to I. Mazer, account no. 244074. In fact, I. Mazer did not have an account with this bank. Nevertheless, American National Bank credited the account indicated without noting the discrepancy.

28. 790 F.2d 407 (5th Cir. 1986).

29. *Ibid.*, at page 410.

30. H.S. Koh, *Op. cit.*, at page 104 onward.

31. E. Patrikis, *Op. cit.*, at page 642.

between the transferee's name and the account number.[32]

While recognising that some legal systems might stipulate that the banks must check that the transferee's name and the account number agree, the Guide considers that the rapid development of electronic fund transfers also implies that the checks carried out by the receiving banker are limited solely to the account number.

Technical developments appear to support this. Checking the transferee's name can prove impossible with batch processed instructions[33] or in the case of card transactions from automated teller machines or point of sale terminals.

It could remain possible to check the agreement of certain orders involving particularly large sums or those which are transmitted individually.[34] The *Legal Guide* appears to prescribe limitation of the scope of the receiving bank's control procedure, and, therefore, that the risks should be borne by the sending bank – at least for orders involving limited sums.[35]

This recommendation simply highlights a trend which is repeated in various subsequent UNCITRAL documents.[36]

The new Article 4A of the Uniform Commercial Code,[37] which has already been adopted by twelve American states, stipulates in a series of very complex provisions (sections 207 and 208) that a bank may rely only on the account number in order to identify the recipient of the order, without being required to determine whether the name and account number describe the same person. However, the bank in question must not be aware of any discrepancy between the name and account number.

Influence of interbank networks and their regulations

It is not possible to discuss the existing interbank provisions in detail here, but several general trends may be indicated in the distribution of liability for error or fraud between the network provider and the participating financial institutions. SWIFT unarguably provides the most detailed regulations in this respect (see below).

Liability of the clearing house or network provider

The CHIPS rules (rule 15) stipulate almost total exculpation and note that:

> . . . the Clearing House shall have no liability whatsoever to any participant or any other person for any loss, liability or expense suffered by such participant or person arising from the Clearing House's acts or omissions in connection with the system including without limitation a loss resulting directly or indirectly from a failure to store, release, authenticate or otherwise process a payment message or administrative message, from an error caused by the system, from the system's failure to record properly a bilateral limit (or modification thereof) or failure to calculate and record properly a debit cap. . . .

The only exception to this exculpation is the case of fraud committed within the actual system. This is covered by an insurance policy taken out by CHIPS to a maximum ceiling of $25 million per incident (rule 16b).

However, in a general manner, CHIPS is releasing itself from liability in the case of an error resulting from the actual system. This must be directly borne by the participants, on the basis of the average daily use of CHIPS. The same is true in the case of fraud committed within the actual system, where the amount exceeds the 25 million insured (rule 16b).

One very telling example cited by M. Lingl[38] can be used to measure the scope of exculpation, whereby a $5,000 transfer becomes $1 million following a system error. If the receiving bank releases the amount to the 'pseudo' transferee before it is notified of the error, it (or the participants) will have to bear the damages.

In contrast, *SWIFT* accepts limited liability where the promised services are not delivered. It is understood that this liability starts the moment the message is accepted by the network and lasts until it is delivered to the receiving bank. Article 21.5.1. of the 'SWIFT II Policy' clearly indicates:

> SWIFT is responsible for the complete international network. Looking at this from the user's point of view, it means that SWIFT is responsible for the message from the time it reaches SWIFT-owned equipment.

Explicit undertakings are made in relation to the quality of the services provided:

> – *rapidity*: the order of the messages is allocated a priority level which corresponds to the urgency of the transmission (Article 18.3; see also 22.4.3);
> – *security*: this involves ensuring both the *integrity* and *confidentiality* of messages, and is demonstrated, in particular, by
>
> – procedures relating to connection to the network (Log-in function: Article 17.1)

32. UNCITRAL, *Legal Guide*, at page 37 onward.
33. *Ibid.*, at page 127 onward.
34. *Ibid.*, at page 128.
35. *Ibid.*, at page 128; see also H.S. Koh, *Op. cit.*, at page 104.
36. See A/CN.9WG.IV/WP.49 8 October 1990, at page 47 onward. If the transferee is described in both words and numbers, and if there is a discrepancy between the two, the transferee's bank should notify the sender.
37. Federal Register/Vol. 55, no. 194/5 October 1990/Rules and Regulations at page 40.
38. *Op cit.*, at page 634.

- the message encryption undertaken by SWIFT
- message numbering (Article 18)
- error detection[39]

- *availability* of the service, which is, in principle accessible seven days a week and 24 hours a day (chapter 4). This is demonstrated by the major back-up systems which have been implemented (Article 21.6).

SWIFT's liability is limited in two ways. First SWIFT is responsible only for direct damages, that is to say for the loss of the amount stipulated in the message and for the resulting loss of interests. The conditions under which this liability may be applied are specified in minute detail (Article 23.4.2):

- negligence on the part of SWIFT in the performance of the promised services or security measures;
- fraud committed by SWIFT employees or contractors responsible for operating the system and fraud committed by *third parties* (persons neither directly nor indirectly employed by SWIFT), namely persons for whom SWIFT is not responsible, but for which SWIFT bears the risk.

However, for SWIFT to be liable, the users must have fulfilled the rules and procedures stipulated in the User Handbook.

Second, SWIFT's liability has a fixed ceiling (Article 23.4.3). In principle, this is B.Fr. 3 billion in the case of a direct loss resulting from fraudulent or dishonest acts committed by SWIFT employees. The same ceiling generally applies to errors or failures arising from within the actual system (see Article 23.4.3 for further information), although a retention of B.Fr. 2 million is borne by the user.[40]

Both systems stipulate a more or less traditional *force majeure* clause which prevents the system manager from being held liable for events beyond its control, particularly those caused by the public utilities (particularly the PTT), catastrophe, political strife, and so on. Nevertheless, it is interesting to note that the network provider feels obliged to ensure the *continuity* of the service and to limit the effects of *force majeure* (the SWIFT example shows the importance of contingency plans). If it is not necessarily negligent to suspend fulfilment of obligations following a case of *force majeure*, it is, on the other hand, negligent not to take all the necessary steps to prevent or limit the effects.

Responsibility of the participating institutions

Here, again, SWIFT provides an interesting example of the type of obligation which might affect the network members.

The participants are responsible for the content of their messages and for the transmission between their terminal and the regional concentrator (see Article 21.5.2).

(1) SWIFT *imposes* an *obligation of availability* on its participants which is manifested on two levels:

- requirements relating to opening hours or times at which messages can be received (Article 21.3 imposes a minimum of seven hours per day between 8.00 am and 6.00 pm;
- requirements relating to back-up measures to be implemented if the main terminal fails (Article 21.6).

(2) In terms of *security*, SWIFT *recommends* that its participants encrypt messages until they reach the regional processor. SWIFT *imposes* authentication in certain cases and for certain types of message (Article 22.1.2.2).

(3) As far as system failures and delayed transfers are concerned, SWIFT stipulates in detail the obligations and liabilities applicable to the various parties (see Articles 22.3 and 22.4). It is interesting to note the emphasis placed on the *obligation* of the participants to *respect a degree of standardisation* prescribed by SWIFT and on an *obligation of heightened diligence* (obligation to notify rapidly any defect in the system and to react rapidly to notices from SWIFT indicating a defect in the system).

(4) A system such as SWIFT comprises three stages based on the apportionment of risk. The sending bank bears the risk until the message is delivered, SWIFT covers the period from delivery of the message until it is transmitted to the receiving bank, which is then liable once the message is received.

Much more could be said on the role of SWIFT as a standardisation platform; guardian of records (Article 22.1.1), certifier or even arbitrator.

Conclusions

Flaubert said that ineptitude consists of jumping to conclusions. The author is not going to risk a definitive opinion on a subject which is in a state of constant flux. Several important ideas, however, may be highlighted.

(1) The obligation of security – the obligation to implement reliable systems is a major principle within the field of EFTs.

39. See the explanation to Article 22.2.1: in concrete terms, the sending bank makes contact with the SWIFT network via the *log-in* procedure using a secret password which enables SWIFT to identify the sender. The sender then sends a message with an *authentifier* (a telegraphic key which guarantees the origin of the transmitted data). The integrity of the message is guaranteed by the *checksum*. When the message is received, SWIFT sends an *acknowledgement*.

40. See Article 23.5 for information relating to indemnification of the loss of interests resulting from delayed payment.

(2) It is apparent that as systems become ever more technically complex, the basis for liability is also developing, and must be judged in terms of risks to be shared, rather than in terms of fault to be established. This in turn raises new questions. Are contractual exceptions to the distribution of risks acceptable? Does *force majeure*, which plays an exculpatory role in relation to fault, continue to play this role if liability is based on risk?

The concept of risk is linked to a more weighty liability borne by the banks. This involves the idea of a *presumption of liability* towards their customers or even of a *responsibility of the transferring bank* towards the transferor for any incident which might occur on the network. The *objective liability* of the banks or *no-fault liability* is also frequently mentioned.

None of these concepts is new. Many of the legal questions discussed (foreseeability, privity, and so on) are no longer new, but are multiplied and brought to light once more by the use of new information technologies which are becoming ever faster, more complex and involve an increasingly large number of actors.

Continual evaluation of the existing rules in the light of new situations – this is the work of the lawyer.

Selected Bibliography

B. Amory and X. Thunis, 'Authentification de l'origine et du contenu des transactions sans papier et questions de responsabilité en droit commercial', Litec, 1987, pages 69 to 115.

B. Amory and Y. Poullet, 'Les relations contractuelles banques entreprises entourant la mise à disposition de services télématiques bancaires', *Banca e Borsa*, 1988, pages 350 to 385.

A. Arora, *Electronic Banking and the Law*, IBC Financial Books, 1988.

E. Bergsten, 'Legal aspects of the International Electronic Funds Transfers', *R.D.A.I.*, 7/87, pages 649 to 668.

A. Bruyneel, 'Le virement', in *La Banque dans la vie quotidienne*, Ed. du Jeune Barreau, Brussels, 1986, pages 370 to 450.

D. Carton, 'Aspects juridiques des ordres de virement transmis par télex', *D.I.S.E.P.*, October 1985, at page 4.

C.N.U.D.C.I., 'Commentaires relatifs au projet de loi type sur les virements internationaux', Report of the General Secretary, 18 September 1989, A/CN 9/WG IV/WP 44 (53 pages).

E. de Lhoneux, 'Télématique et droit monétaire', in *La Télématique*, Story Scientia, Ghent 1985, vol. 2, pages 287 to 302.

R. Goode, *Electronic Banking*, London, 1986.

J. Jetton, *'Evra Corp. v Swiss Bank Corp.*: consequential damages for bank. Negligence in wire transfers', *Rutgers Computer and Technology Law Journal*, 9-1983, pages 369 to 402.

S. Karageorgiou, *Electronic Funds Transfers*, Technical & Legal Overview, thesis, London, 1990.

H.S. Koh, 'Liability for Lost or Stolen Funds in cases of Name and Number Discrepancies in Wire Transfers: Analysis of the Approaches Taken in the United States and Internationally', 22 *Cornell International Law Journal*, 1989, page 98 onward.

H.F. Lingl, 'Risk Allocation in International Interbank Fund Transfers: CHIPS and SWIFT', *Harvard International Law Journal*, vol. 22, no. 3, Fall 1981, pages 621 to 630.

Y. Poullet and X. Thunis, 'Réflexions sur le mouvement électronique de fonds', in *La Télématique*, Story-Scientia, Ghent 1985, vol. 2, pages 259 to 271.

Y. Poullet and G. Vandenberghe (eds), *Telebanking-Teleshopping and the Law*, Kluwer, Deventer, 1988.

M. Schauss and X. Thunis, 'Aspects juridiques du paiement par carte', Cahier du C.R.I.D. no. 1, 1988, page 125.

H.S. Scott, 'Sur les transferts interbancaires par télétransmission aux Etats-Unis', *R.I.D.C.*, 4-1985, pages 967 to 984.

D. Syx, 'Le transfert électronique de fonds: le droit hésitant face à une réalité galopante', in *La Télématique*, Story-Scientia, Ghent 1985, vol. 2, pages 221 to 249.

M. Vasseur, 'Aspects juridiques des nouveaux moyens de paiements', *Rev. de la banque*, 1982, page 592 onward.

M. Vasseur, 'Le paiement électronique. Aspects juridiques', *La Semaine Juridique*, 1985, I, 3206.