Legal Aspects of Electronic Funds Transfer

Antonio Millé


1. CURRENT STATE OF MONETICS

At the beginning of civilization, in the search for an appropriate procedure to carry out the essential barter for trade, our ancestors arrived at the choice of certain precious assets as accounting unit. Expansion of trade, together with the organization of the State, later led to «fiat money» being issued by the sovereigns, stamped and guaranteed by the issuer. Subsequently, «scriptural» or written means of payment made it possible to substitute the physical delivery of metallic money or paper money by a letter or written order given to a third party, to credit said amount to a specific account or to deliver said values to the bearer claiming them.

«Monetics» is a new development in the field of scriptural means of payment, evidenced by the substitution of payment orders set out on paper by others based on informatic devices and which are, therefore, recorded mainly on digital records and the transfer is currently done through electronic means.

In the present state of the art, which will be considered in this work, the Electronic Fund Transfer (hereinafter referred to as «EFT») takes place through:

a) Automatic Teller Machines (ATM);
b) Points of Sale (POS);
c) Home Banking (HB).

The emergence of new instrumental basis and procedures for the transfer of money orders has resulted in non-traditional legal problems connected with EFT requiring different and imaginative solutions. Nevertheless, as it will become evident in this work, I do not believe that we are faced by a new legal approach of the evolution of the means of payment is discussed in El aspecto legal del dinero by F. A. Mann, Mexico, 1986. Its course towards «electronic money» in The Cashless Society, by August Bequa, New York, 1981.

2. «Monetics» is an appropriate neologism coined by the French worshippers of the Droit de l'Informatique. M. Vivant and Ch. Le Stanc define it as a «system for payments based on transfer mechanisms in which informatics plays a role» (LAMY Droit de l'Informatique, Paris, 1987, p. 1332).
kind of money or by a legal vacuum that is difficult or impossible to fill by the currently available legal means.

It should be noted – and this is frequently overlooked by authors dealing with this subject – that legal problems related to EFT (at least with regard to ATM and POS) are directly related to the use of plastic cards as means of accessing a system and identifying an account owner. Cards, originally restricted to payment and credit functions, fall within a legal category with inherent problems and solutions, not necessarily linked to informatics and telematics, to whose generalization they proceeded. It should be remembered that many of these problems and solutions are common to «Monetics» as a whole 1. This is simply an additional manifestation of the trend towards the integration of banking and card business.

2. AN ACTIVITY WITH MULTIPLE PARTICIPANTS

The means of payment evolution, from prehistoric barter to EFT, has resulted in a constant increase in the number of parties involved in these transactions. In the present state of Monetics we must consider as subjects of rights and/or obligations related to EFT:

a) account holders, who may number one or more in each operation (transfers from one user’s account to another’s) who may operate through more than one authorized account owner in connection with the same account (holders of second cards) and also use a single method of accessing the system to operate with different accounts (associated accounts);

b) the bank or institution which opens the account and issues the cards;

c) the bank receiving the transfer ordered by another bank, according to the client’s instructions;

d) the bank responsible for the ATM, through which transactions are made by multiple account owners, many of whom are not its clients;

e) the company providing the physical facilities for the installation of an ATM, whose operation is not controlled by it;

f) the company managing the ATM, POS or HB system;

g) the company providing the physical means of communication to transport signals between terminals, bank computers and central system computers;

h) the bank or institution acting as a clearing house between banks and companies linked to the system, and

i) retailers receiving payment for goods from the public by means of credit or payment cards or POS.

As legal features of the EFT system, as regards the intervening parts, we must point out the following:

3. For an exhaustive study of the problems related to credit and payment cards, including abundant references to comparative law and discussion of this subject as a part of «banking telematics», see La Pratique du Droit des Cartes by A. Bertrand and P. Le Clech, Paris, 1988.
— most transactions involve several parties;
— some of the parties involved in transactions derived from the system are linked to each other by direct contractual relationships, whereas others are only indirectly linked (provisions regarding them, included in an agreement celebrated between two third parties) and others are not connected to each other by any contractual links whatsoever.

In this general and not exhaustive review of legal problems related to EFT — the only purpose of this paper — we cannot consider but the more relevant problems affecting banks or companies issuing credit cards in their relations with users and third parties acting fraudulently. The variety of relationships resulting from the number of parties already mentioned, obviously points out the existence of a vaster number of problems which also deserve attention.

3. The Business Legal Framework

A typical feature of Fiat Money is that the legislation which governs it is part of Public Law, whereas provisions which rule scriptural means of payment — since they do not affect the State’s interests — are found mainly in Private Law. Nevertheless, the substantive provisions governing EFT lie within the field of contractual regulations. Thus, we see an increasing participation by interested parties in the management of the instruments of payment and an increased predominance of private conventions over general rules of law.

In the Latin American region, whose civil legislation is inspired by the principles set out in the «Napoleonic Code», a common principle states that «dispositions set forth in an agreement constitute a rule for the parties, to which they must submit as if it were the law itself» 4. All issues set forth in the agreement, not governed by the private convention, are to be governed by the basic rules of law. Thus, the importance of contracts in governing the legal relations resulting from EFT can be easily understood.

From the standpoint of this paper, the most important conventions governing EFT are:

a) the contract between a bank or company and the organization managing an ATM, POS or HB network;
b) the contract through which a bank or company agrees with the user the opening of an account or the issuing of a card, and
c) the contract between a business enterprise accepting operations with a credit or payment card or a POS and the company managing a credit or payment card system or a POS network.

4. Article 1197 of the Argentine Civil Code, based on the article 1134 of the French Civil Code.
Although civil law regimes generally include provisions similar to those in article 1149 of the Argentine Civil Code, wherein it is stated that «contracts cannot be enforced against third parties nor can they be invoked by them...», contracts governing EFT usually include provisions which not only refer to relations between the executing parties but also establish a link between one of the parties (the owner of the account, for example) with the counterpart of the other party, under a different contract (the retailer, in our example). Therefore, in spite of the already mentioned general principle, since these stipulations are freely assumed undertakings of the contracting parties, such stipulations are fully valid and enforceable.

As regards the regulatory framework applicable to EFT, it should be remembered the penetrating comment made by André Bertrand and Philippe Le Clech that — in spite of the inherent features of each legal system — countries governed by «common law», usually based on the doctrine of precedent, have a more complete network of legal provisions on EFT than countries with a Latin legal tradition, generally based on statutory law.

4. RISK AND INFORMATICS

In the legal field, Informatics has been accepted with certain distrust since it is considered a still not completely developed technology, capable of mal functioning and that the risk involved in its use must be taken by those who profit commercially from it. In fact, this doomsday view is inconsistent with current technology, which has proven to be highly safe as regards equipment devoted to EFT and particularly as regards devices dedicated to EFT operations, whose physical and logical components have been specifically designed to be error resistant.

Nevertheless, the possibility of mal functioning affecting the input, processing, recording or output of EFT operations must be considered. These risks include:

a) Malfunctions caused by the environment: heat, humidity, static electricity, dust, defective power supply, etc., are physical factors capable of causing changes in stored data and, hence, causing defective processing and errors in output. Technical advances tend to decrease the likelihood of such failures, as a result of the adoption of appropriate technical countermeasures (air conditioning, insulation, uninterrupted power supply, etc.).

b) Equipment failures: certain components of computer equipment (particularly mechanical elements, more likely to fail due to friction and wear) may fail and this risk is increased by improper maintenance. This is particularly


162
true in the case of printers where quality control standards are difficult to apply and improper functioning could lead to failure to print or credit an operation due to lack or break in printing paper or ribbon. These risks are lessened by control systems which prevent the defective operation of equipment and the duplication of records which are stored in the magnetic memory not printed on paper.

c) Errors in design architecture: theoretically, the conjunction of physical and logical components in a system, subject to operating in an infinite combination of variable circumstances could, in some of them, generate errors in results or output. In fact, both hardware and software driving ATM, POS and HB network are products that have been tested in a great number of installations, where millions of transactions take place. In the present state of practical experimentation of systems, the possibility of an unexpected error due to the conjunction of unforeseen factors is extremely unlikely.

d) Human errors: involuntary errors (or wilful misuses) caused by operators when loading, processing or erasing data, working with certain files, using certain communications protocols, etc.

e) Errors in data collection: exogenous errors, prior to inputting data. Experience indicates this is the most important source of risk. Although data entry processes have a high safety margin (validation procedures), the input of erroneous data is inevitable. Once the information has been stored (or worse, after having been processed) it is extremely difficult to detect and correct. It should be pointed out, however, that data transmitted over EFT systems remains, in most cases, unaltered after the original input and is not an element in subsequent process after collection. This increases its reliability and evidently decreases the possibility of errors, making the control of processed information far more transparent.

The above mentioned failures may cause problems which have very serious legal consequences for the various parties participating in these transactions. Briefly, they include:

a) Problems related to user identification: leading to the rejection of orders or instructions given by the legitimate user, as well as processing of operations initiated by unauthorized users.

This includes the serious risk of wilfully improper use by someone forging or altering cards or using fraudulently obtained identification codes, who link up to the system and cause harm to the various interested parties.

The constant improvement of security systems tends to decrease this risk which, nevertheless, is one of the most important causes of loss in the exploitation of EFT systems.

b) Changes in information: refers to the possibility of processed information being modified by accident or by fraudulent manoeuvre. As the operation of an EFT system is based on a constant remote processing of information, the deviation from destination constitutes an important factor of risk.

c) Delays in message transmission: losses and damages can result from delayed transmission of operations or the late compliance with instructions. EFT te-
chniques do not always offer the user an opportunity to verify the timely performance of operations.

d) Disappearance of information: information can disappear during input, transport, processing or storage, causing damages to those entitled to claim a benefit following the correct processing of data.

5. Problems related to evidence

The current legal system witnesses a technical stage of development in which transactions take place between individuals who face each other, or at a distance – based on evidence set out on paper, usually signed –. Informatics manifestly tends to eliminate paper as a foundation for transactions being processed and telematics eliminates the need for the physical presence of the actors. EFT (based on informatics and telematics) was obviously destined to clash with a legal structure which corresponded to a paper based culture, relying on instruments and signatures.

In this sense, the most critical legal considerations are related to the identification of the parties involved in a transaction, and to the value of records on electronic memories as legal evidence.

The method used by an ATM or POS system to identify an account user has been a physical device (a card) with a confidential code recorded (the Personal Identification Number - PIN) to be validated by the system when verified against the account and card numbers.

HB techniques, since they are based on telephones, «Minitel» type terminals or computers, use only a PIN which, for safety reasons, usually includes eight digits.

Constant efforts are being made to implement techniques substituting cards and PIN in order to identify those who operate with EFT. Voice recognition, fingerprints, blood vessels on the retina, etc., are some of the methods suggested in connection with identification based on the anatomical structure. Static or dynamic analysis of signatures appears to be a less feasible method from a technical standpoint but closer to our traditional legal formalities. None of these methods has prevailed to date and its efficiency appears, in practice, surpassed by other less costly and complicated methods, such as the «intelligent» card whose memory include – besides data on current account management and statement – resources directed to identification. 7

Another serious legal problem relates to the evidence of EFT transactions. Electronically conducted business, just as any other form of business, may result in controversies among the parties, who may claim to have never effected a transaction or that they wished to engage in different operations or

7. A plastic card with imbedded electronic microcircuits, which acts as microprocessors and memories, experimentally used in the French «Carte Bleu». 164
who dispute the amount, opportunity or any other related circumstances. The facts of the matter will be established and the correct interpretation thereof will be possible under law only if adequate evidence is available. Said evidence, to be useful, must be both legally admissible and materially convincing.

Electronic expression (not perceivable by human senses) and magnetic media, inherent to EFT, is more a problem of formal adjustment to regulations than something involving the essence of evidence. Electronic evidence, in the absence of unavoidable procedural requirements, can meet standards of clarity, unchangeability and permanence when reproduced by appropriate technical means and set out in unerasable basis.

As a matter of fact, the main legal problem in this regard is the imbalance among the parties, due to the fact that one of them has absolute control over the recording and storage systems and the other must rely on the devices controlled by his opponent in the event of a dispute. A basic legal principle indicates that each claimer is concerned with the evidence of what he is claiming, thereby forcing an EFT user (whose hypothesis of conflict would have as a probable opponent the manager of the system technical devices) to trust in the technical perfection and good faith of this potential opponent to certify his statements.

Different techniques have been used to attempt to balance this uneven situation as, for example, the automatic issuing of paper certificates before the definitive processing of the transaction by the ATM or with the presence of one or more officials while opening envelopes containing deposits made through automatic terminals.

In this case also, it would appear that the use of cards with memory which constitute a means of evidence in the hands of the user — is a possible solution, in the present state of the technique.

Since very few countries have appropriate legislation on this subject, problems related to the identification of the operator and the evidence of these sorts of transactions have been solved by provisions contained in the parties' contracts.

When funds are withdrawn from an ATM, a purchase is debited at a POS (point of sale) or funds are transferred through HB (home banking), the user is linked up to the system and communicates with a computer by striking or tapping a keyboard; there is usually no human intervention, except by the

8. Interested readers will find striking views on the problem of evidence and informatics in the records of lectures and debates organized by the Association Française du Droit de l'Informatique, titled L'Informatique et le Droit de la Preuve, Paris, 1986.

9. The United States of America enacted on this issue the Electronic Fund Transfer Act, approved in November 10, 1978 as title XX of the «Consumer Credit Protection Act». In Denmark, a «Law on payment cards» touching on some aspects of this issue has been in force since January 1, 1985.
user and, therefore, it seems inappropriate to refer to accordance, which is one basic aspect of any bilateral agreement.

Nevertheless, there must have been a prior occasion when we spoke to another human being - to sign papers and execute the agreement which led to the opening of an account or the issuance of a card, which set out in minute detail the stipulations under which we would operate in the future. It is in these agreements or contracts that the parties stipulate the requirements for acknowledging an instruction or signature and what evidence of an operation will be accepted as valid. The problem with these clauses is that some legal scholars construe them as affecting principles of Public Policy and, therefore, being null and void, since those principles cannot be modified by private agreements 10.

This, in turn, leads us to a really important legal consideration since evidence must, under law, be weighed from a formal point of view (rules regarding introduction of evidence as proof of an act) as well as from a material standpoint (the degree of credibility of evidence submitted). Since certain legal systems specify what can be validly used as evidence and the value assigned to each method of proof 11, the enforceability of conventions regarding evidence must be analyzed very carefully, particularly as regards the enforcement of obligations set out in documents and signed as proof of a certain legal act 12.

Although Informatics and Telematics have been benefitted by the application by analogy of legal principles originally enacted to regulate situations occurring in a previous technical culture, the inherent rigidity of formal rules nevertheless precludes interpretation by analogy 13 and demands an urgent decision on the part of the legislator regarding instruments and evidence of legal acts according to the current state of the facts.

6. PROBLEMS RELATED TO CIVIL LIABILITY

Experience derived from the use of EFT systems allows to define some critical areas related to risks which could result in civil liability 14. A brief list must include:

10. This is the opinion of the Colombian academic, Mr. Hernando Davis Echaodia, who believes that it is not acceptable that the parties impose on a judge rules on how to assess facts on which he rules (Teoría General de la Prueba Judicial, Buenos Aires, 1981, T. 1, p. 517).
11. System called 'legal evidence' as imposed by Colombian rules of evidence or less strictly by Venezuela. It is the opposite of "freedom of evidence" wherein the parties and the judge may use any appropriate means as evidence, as adopted by the Argentine procedural law.
12. Civil laws inspired in the Napoleonic Code reflect (as the Argentine Civil Code does, in Art. 1193) the principle set out in its Art. 1341 which demands that any legal act whose economic importance exceeds a set amount (currently FF 5000 according to the French law and amount which cannot possibly be expressed due to inflation, in Argentine law) be evidenced by written document and signed.
13. As cleverly pointed out by Alain Bensoussan in this address during the meeting mentioned in note 10.

6.1.1. Risks related to the creation of means of access:
It is the inherent risk of manufacturing physical media (cards) and assigning logical media (codes) not only by banking and financial institutions handling the accounts but also by companies involved in the production of physical inputs. The usual causes of risk are negligence or fraud by the staff themselves, which could result in violation of the confidentiality of codes, or in the appropriation of physical media by third parties.

6.1.2. Risks related to the issuing of physical means of access:
Another frequent cause of damages is the distribution of cards to persons who did not request them, and the use of standard mail or postal services to send cards to those who requested them. In the first case, anyone who is not aware of having been chosen, without being asked, to become a card holder, is unable to take steps to prevent their improper use by third parties. In the second case, when a card is stolen before being delivered to the addressee, the latter is also equally incapable of protecting his or her best interest.

6.1.3. Risks related to protection of means of access:
This is a risk assumed by the user of the system, who must keep the physical means under safe custody and protect the confidentiality of the logical means, so that they remain unknown to third parties. Experience indicates that a large number of users fail to fulfill both obligations and that an incredibly large number of them write down their access code on the card itself or a piece of paper carried together with the card. By making illegal maneuver easier, through carelessness, the user is also obviously liable. This responsibility is increased when the user does not bother to take the time to fulfill his prescribed obligations, in the event of loss or theft.

6.2. Risks Related to Equipment Malfunction.
This section should include all liabilities derived from mistaken or defective operations due to technical factors. In spite of reliability of the equipment, it seems appropriate to point out the current vulnerability of communication systems and the growing number of «hackers» in informatics-related crime, factors which constitute an external risk and whose responsibility cannot be attributed to any of the parties participating in the relationships under consideration.

6.3. Risks Related to Failure to Follow Certain Routines.
This refers to the responsibility of merchants who perform operations paid by electronic means. They have the obligation to perform certain checks and request, certain approvals and must, therefore, bear the responsibility of damages resulting from failure to perform or the improper performance of those procedures.

6.4. Risks Related to Failure to Perform or Delayed Performance of Instructions.
This is a type of damage usually associated to HB operations and does not really differ from identical non-electronic operations. The delayed or incorrect transmission or processing of instructions can result in the late payment of a bill submitted by a third party, or in financial operations performed at an undesired rate, etc. The truly unique feature of the problem is that in case, as in many of the other cases discussed, the user of EFT has difficulty in evidencing the manner and the occasion on which he instructed certain operations to be performed.

7. Problems related to fraud

EFT systems have certain unique features related to specific legal problems resulting from illegal acts. EFT frauds can be classified in two large groups:

7.1. The Improper Use of the System
In practice this is done by the account or card holder using the original physical and logical means of identification, and the improper use is reflected in a behavior which violates the stipulations between the parties on the use of the systems.

7.1.1. Operations exceeding the authorized limit. A distinction must be drawn between the hypothesis in which the balance due is eventually covered by the user and that in which the user fails to pay his debt. In this last case an additional distinction comes into play: when the balance due is equivalent to expenditures consistent with the life style of the user as distinguished from those reflecting a disproportionate increase in expenditures, which can be considered as evidence of a fraudulent manoeuvre. Courts have found this to be a crime.

7.1.2. Operations with expired card or card which have been removed from circulation. These operations are criminal when performed with the intention to defraud.

7.1.3. Prohibited operations: one of the most frequent is to disguise cash loans under the appearance of sales made by stores linked to the system.

7.2. Assumptions of Fraudulent Use
Cases where the EFT is used by third parties as the appropriate instrument to commit a crime. The most frequently used methods are:

7.2.1. Fraudulent opening of an account: in these cases the author of illegal acts is the true card holder, who opened an account, usually under a false

15. For a view from the standpoint of the Argentine Criminal Law, see Fraudes con tarjetas, by ANTONIO MILLÉ in América Latina y la Monetica, Buenos Aires, 1989, p. 47.
16. For example, the decision handed down by the Cámara Nacional Criminal y Correccional (Buenos Aires), Sala III, February 12, 1982 in re «Tepper de Edelstein, N.» See Tarjetas de Crédito by JOSÉ LUIS AMADEO, Buenos Aires, 1984, p. 27.
identity, with the only purpose of defrauding (ordinarily through standard operations and subsequent failure to pay).

7.2.2. Illegal use of cards by someone who did not obtain it fraudulently: a very common crime. The authorized user entrusts the means of access to the EFT to someone (usually relatives or employees) who perform illegal acts with them.

7.2.3. Theft and robbery of physical means of access: at present, a very common crime. Cards providing access to ATMs and POS have become the favorite targets of individuals and international criminal organizations.

7.2.4. Forged cards: a crime committed by those who modify lost or stolen cards (by «ironing» them) and by those who manufacture «valid false cards». This activity is one of the most painful headaches in this field.

8. Conclusions

After reviewing the EFT phenomenon in the light of current statutes, certain conclusions become evident:

1) First, one of the most striking aspects is the fact that such a widely used system, processing daily millions of transactions for a total of truly enormous amounts, is not subject to greater problems or failures, to the point that it is sometimes difficult to find information on problems, when legal scholars try to examine the facts that could be related to several theoretical hypothesis revealed during a review. This supports the high degree of reliability of the physical, logical and communication means and devices used for EFT and the effectiveness of practices and routines adopted to systematize the operations.

2) Stipulations between the parties prevail over legal regulations, coinciding with an almost universal use of them, thereby seeming to impose a standard in this regard by encompassing very different and broad areas of law, which are clearly differentiated in other issues of law.

3) It is clear that background regulation referring to currency, usual credits and contracts has been sufficient, as an additional framework to that of private stipulations, for regulating the EFT phenomenon. Nevertheless, regulations referring to instruments and evidence of these acts, are not equally adequate and pertinent and they deserve specific analysis and reform or amendment.

4) It is similarly evident the need for changes in criminal law to adjust to crimes committed through electronics means and for the protection of values incorporated by Monetics into modern social life.

5) All antecedents make it foreseeable that developments of techniques, most likely based on cards with memory, make it possible to overcome those problems related to user identification and evidence of transactions, without a major deviation from the classical principles on instruments and evidence.