UNITED NATIONS

GENERAL ASSEMBLY

Distr.
GENERAL

A/CN.9/250/Add.4
19 April 1984

ORIGNAL: ENGLISH

UNITED NATIONS COMMISSION ON
INTERNATIONAL TRADE LAW
Seventeenth session
New York, 25 June - 11 July 1984

# DRAFT LEGAL GUIDE ON ELECTRONIC FUNDS TRANSFERS

## Report of the Secretary-General

(continued)

Chapter

on

## FRAUD, ERRORS, IMPROPER HANDLING OF TRANSFER INSTRUCTION AND RELATED LIABILITY

CONTENTS



V.84-85182

## Introductory note

1. The volume of electronic funds transfers and the sums involved suggest that the potential losses could exceed the losses experienced with paper-based funds transfers. At the same time customers of banks have been concerned that the move from paper-based funds transfers to electronic funds transfers would result in their bearing a larger share of any losses arising out of errors or fraud. The result has been an unusually unsettled state of the law as the participants have attempted to establish appropriate grounds for assigning loss in the multitude of new and rapidly changing factual situations. The problems would be difficult enough if only the banking law governing the responsibility of various parties to a funds transfer were involved. In spite of the many years during which such problems have been considered in regard to paper-based funds transfers, there remain a surprising number of unanswered questions in many legal systems. Moreover, the changes in procedures necessitated by the use of electronic techniques raise questions as to whether the rules on liability for paper-based transfers should be applied to electronic funds transfers.

2. The problems are complicated by the rapidly changing role of the telecommunications carriers and the pressures on the law governing liability which have ensued. Whereas previously telecommunications were a service external to the bank offered by a common carrier monopoly, today the office equipment in many banks is linked in local area networks, branches are linked by dedicated lines and banks are transmitting an increasing share of their funds transfer messages to other banks by telecommunications. Telecommunications are no longer external to the bank; they have become a vital internal operating medium, as they have in many other fields of economic activity. Because of the blurring of the lines between computers and telecommunications, the former monopoly of telecommunications service has been broken in some countries and is under pressure in others. As a result of these developments, questions are being raised as to whether the former (and largely still existing) exemption from liability accorded to the telecommunications carriers is still a valid policy.

3. This chapter considers first some of the factors which contribute to the occurrence of errors or fraud in electronic funds transfers and the actions that can be taken to minimize their occurrence. Secondly, it considers the allocation of the loss among the various parties to the funds transfer. Then, the focus is on the extent to which and the party from whom the bank customer as transferor or transferee can recover losses suffered as a result of an improper handling of transfer instructions.

## A. Fraud

### 1. Opportunity for fraud

4. Fraud in an electronic funds transfer involves an unauthorized instruction, alteration of the account to which an entry is to be made or

alteration of the amount of the entry. To avoid losses from fraud, adequate steps must be taken by the party in a position to do so to prevent unauthorized instructions from appearing as though they were authorized.

(a) Dishonest employees of bank customer

5. Many losses due to fraud in electronic funds transfers are caused by the application of techniques well known in connection with paper-based funds transfers. Three common examples involve dishonest employees of the bank customer.

6. A clerk charged with preparing the payroll or preparing the vouchers authorizing payment to a supplier may falsify the payroll or the vouchers so that payment is made to a person not entitled to receive it. If payment is made by means of a cheque, the dishonest employee gains possession of the cheque and, after endorsing it in the name of the fictitious person, deposits it in an account he has previously opened in that name. If payment is made by means of a paper-based or electronic credit transfer, the funds are credited to the account of the fictitious person in due course. The fraud is completed by the subsequent withdrawal of the funds from the account by the dishonest employee.

7. If the dishonest employee has the authority to authorize the funds transfer on behalf of his employer, rather than the responsibility of preparing the substantiating documentation, he signs the cheques or paper-based credit transfer instruction or authorizes transmission of the data in electronic form to the bank. The fraud is completed in the same manner by withdrawal of the funds by the dishonest employee.

8. In both cases, the funds transfer instruction appears to the bank to be genuine and authorized, although it is fraudulent in fact. These cases have caused considerable difficulties in some countries when the funds transfer instruction was in the form of a cheque, since the completion of the fraud requires the endorsement of the cheque by the dishonest employee in the fictitious payee's name. Nevertheless, the endorsements of the dishonest employee (or of his accomplice) have usually been held to authorize the bank to honour the cheque.

9. The allocation of the loss to the bank customer causes fewer doubts when the fraudulent payment is by paper-based or electronic credit transfer, since the fraud does not require any equivalent of a forged endorsement.

10. A third type of fraud by a dishonest employee who has no authority for issuing funds transfer instructions on behalf of the employer is possible when a computer terminal located at a bank customer's place of business can be used to make funds transfers. If the dishonest employee is able to gain access to the terminal and learns how to enter a funds transfer instruction, including the necessary password or other security measures, the instruction will be followed by the bank. For many countries this is a new form of fraud which could not be committed in a paper-based funds transfer. However, in some countries which permit the use of mechanical forms of signature on cheques or

paper-based credit transfer instructions, a similar problem arises when a dishonest employee (or third person) gains access to the mechanical signing apparatus and causes cheques or credit transfer instructions to be issued payable to himself or to a fictitious person.

11. In those countries which do not prohibit mechanical signatures, it seems to be the general rule, often reached by agreement between banks and their customers, that a bank which honours in good faith a cheque or credit transfer instruction signed fraudulently by a genuine signature apparatus can debit its customer's account. Although different legal theories might be used to support such a result, the underlying reasons are that the bank cannot distinguish a genuine usage of the signature apparatus from an improper usage, the bank customer has a responsibility to guard carefully an apparatus which can so easily be used fraudulently, and the bank customer is negligent in allowing the signature mechanism to be used fraudulently.

12. The reasons for allowing the bank to debit the customer's account in the case of a fraudulent use of the signature apparatus would also apply to the right of a bank to debit its customer's account for the amount of fraudulent funds transfer instructions made by use of a computer terminal located at the customer's place of business. However, it should be noted that the responsibility for security over the terminal at the place of business of a bank customer is shared by the bank customer and by the bank necessitating an allocation between them of that responsibility and of a failure to exercise it adequately.

### (b) Fraudulent use of customer-activated terminals

13. Terminals located at the place of business of a bank customer as well as automated teller machines, cash dispensers, point-of-sale terminals and home banking terminals share the characteristic of being customer-activated. One of the purposes of a customer-activated terminal is to eliminate the need for human intervention on the part of the bank. This has the effect of reducing the likelihood of error by the bank in processing funds transfer instructions. However, the use of customer-activated terminals also has the effect of increasing the possibilities for fraud.

14. All computer terminals which can authorize a funds transfer work in essentially the same way. Before an individual can use the terminal, he must first establish his authorization to do so. A bank employee may log-in one time to establish his authority to use the terminal for the day. A customer-activated terminal would normally require separate authorization for each transaction, unless it was in constant use by the customer. A given terminal or customer may also have a limit placed on the types of transactions which can be authorized, the accounts which can be debited or credited and the monetary amount, which may be calculated per transaction, per day or in any other relevant way.

15. The log-in or authorization procedure to be followed before a customer-activated terminal can be used is established by the bank. In deciding on the procedure to be followed, the bank (or the electronic funds

transfer network of which the bank is a member) must balance considerations of safety, cost and customer acceptance. Usually, the more secure the authorization procedure, the more expensive it is for the bank to install and maintain and the more difficult it is for customers to use. For marketing reasons it may be desirable for the customer-activated terminal to be user-friendly, but a user-friendly terminal also tends to be intruder-friendly. This is a delicate balance for the bank to make, and it is a balance which changes as technological developments occur.

16. Restrictions on the types of transactions which can be authorized or accounts which can be debited or credited can be an effective way to reduce the likelihood of fraudulent transactions. Restrictions on the montary amount have only a limited effect on eliminating the incidence of fraud, but they can be an important means of limiting the financial consequences of fraud. This may, however, be meaningful only in regard to consumer oriented networks since the upward limit in commercially oriented networks may need to be so high that sufficient room for serious fraud is allowed.

17. Current models of cash dispensers, automated teller machines and point-of-sale terminals require the convergence of two items to authorize the transaction, i.e. a plastic card with magnetic stripe containing certain information and the entry by the bank customer of a personal identification number (PIN). New and more secure forms of plastic cards are in experimental use. In some proposed home banking systems it would not be feasible to use a plastic card for authorization purposes; therefore, the authorization procedure depends on a PIN or password alone. A terminal located at a business establishment can have more complicated and presumably more secure procedures, but in essence they usually revolve around the use of passwords and the possible use of a plastic card.

18. There are currently two different approaches used by banks for protecting the security of the PIN. One approach concentrates on eliminating the possibility that an employee of the bank or funds transfer system can know the PIN. The PIN is generated by a computer using an algorithm and certain basic data relevant to the customer. The resulting four or six digit number is inserted by the computer into a sealed envelope and mailed or otherwise delivered to the customer. If properly followed, this method can give a secure PIN for each customer. However, since the number is abstract and may be difficult to remember, many bank customers feel the need to carry the number with them whenever they intend to use their plastic card, thereby seriously compromising the security of the PIN.

19. The other approach attempts to make it easier for the bank customer to remember the PIN by allowing the customer to choose his own number. A customer often chooses a number based on his own or his spouse's birthday, his street address, telephone number or other number already well known to him. While this has the advantage of making it less likely the bank customer will carry the number with him in written form, it has the disadvantage of reducing to a minimum the combination of numbers likely to be chosen by any given person and making it thereby easier to determine what that person's PIN might be. Moreover, the PIN is known to at least several of the bank's employees and, since the PIN is no longer generated by computer, it must be entered into the customer's file and be available to anyone having access to that file.

20. Password security for terminals located in businesses or in homes raises the same kind of problem. The password should be neither so obvious that it could easily be guessed nor so obscure that the user will keep it in written form, unless the writing is to be kept under strict security controls. A terminal from which a wide range of funds transfers can be made for significant amounts of money should be subject to additional safeguards. Log-in might require the concurrence of two different persons with different passwords. Passwords can be changed at relatively short intervals, although that introduces difficulties of their distribution from the bank to the customer, or vice versa. The bank can cancel a password automatically if it is not used for a particular period of time, since this may mean that the person to whom the password is assigned is absent.

21. Protection against fraud in the use of customer-activated terminals is, therefore, a joint endeavor of the bank and the customer. The bank must install and maintain as good a security system as is practicable considering the cost involved and the interference with use which may result. One measure of the quality of the security system is the extent to which the customers of the bank, who are often non-professionals in the use of computers and in funds transfers, follow the security instructions given them by the bank.

### (c) Customer supplied machine-readable instructions

22. A somewhat similar situation exists when the customer supplies the bank or an automated clearing-house, with funds transfer instructions in batch on computer memory device or in machine-readable paper-based form. Although it is the responsibility of the customer to prepare the instructions properly including the use of internal controls to guard against both fraud and error in their preparation, the bank or clearing-house should be responsible for verifying that item counts and value agree with the sums indicated, that they are within the parameters authorized by the customer for such batches, and that the batch otherwise appears to be free from alteration subsequent to its preparation. These controls can easily be exercised by the bank or clearing-house at the time it verifies the devices prior to processing.

### (d) Fraud by bank employees

23. Employees of banks and other entities in the funds transfer system also have access to terminals with which they can enter fraudulent transactions. Fraud by such parties can be particularly difficult to discover unless the bank has a well designed system. The possiblity of a dishonest employee programming the computer to credit his account and to erase all records of the transaction has been well publicized. This should not be possible, however, since the bank's computers can be programmed to leave a complete audit trail of all activity, including instructions to delete transactions. For this to be done effectively, the audit trail should be programmed by different persons from those who prepare the applications programs and should be subject to independent audit.

(e) Fraud by tapping telecommuncations transmissions

24. It is relatively easy to tap any telecommunications system over which electronic funds transfer instructions might be sent. The cost for complete physical security of the transmission system is such that it is not feasible for commercial purposes. Therefore, the design of any electronic funds transfer system should assume the possibility of interception and reading of messages, alteration of genuine messages and the introduction of false messages. The first line of protection against such fraud is encryption. If the encryption standard used is powerful enough, there is no danger of interception, alteration or the introduction of false messages. However, an encryption standard which is highly secure today may be rendered insecure within a few years by the development of more powerful computers and new techniques for factoring the large numbers on which encryption is based. Moreover, the proposals in some countries that a government agency have all encryption keys used for transborder data flows would create a potential weak link in the system of security over which the parties would have no control. The creation of rigorous logs of all in-coming and out-going funds transfer instructions and the assignment of in-put and out-put sequential numbers provide a means of verifying the time of receipt or dispatch of the message and the other party to the message. These procedures increase the likelihood that a fraudulent instruction will be recognized and they are an essential means of subsequently discovering and tracing suspected fraudulent instructions.

2. When may a fraudulent instruction justify a debit to an account

25. Although a bank is normally authorized to debit a customer's account only for the amount of an authorized instruction, it may also debit the customer's account for the amount of certain unauthorized instructions, particularly when the fraud was made possible through the lack of adequate controls on the part of the customer. There is, for example, little doubt that the customer's account can be debited for the amount of fraudulent transfers initiated by those employees authorized to act for the customer, unless there was something about the transaction which was so unusual that it ought to have raised the suspicions of the bank.

26. However, it is less clear whether the bank or the customer should bear the loss for fraud committed by means of a customer-activated terminal. Since the bank designs the basic security and authorization procedures and the customer carries them out, one approach is to assign the loss on the basis of comparative negligence in each case. This approach may be feasible for those cases where it is evident that the fraud was made possible through a clearly inadequate security and authorization procedure or that the customer had been unusually negligent in following those procedures. It is not, however, an efficient means of distributing the loss, particularly in cases of fraud in consumer oriented systems, where the individual loss is often not large enough to support a full judicial inquiry.

27. As a result, there is a tendency to search for formulas of general validity for the vast majority of the cases. Bank-customer contracts, which are normally standard form contracts prepared by the bank, typically authorize the bank to debit the customer's account for any transfer made by use of the particular type of customer-activated terminal when the proper PIN or password and plastic card, if any, was used. In the case of systems in which transfers are authorized in part by use of a plastic card, customer liability normally ceases once the customer has notified the bank of the loss or theft of the card and the bank has had the possibility of entering the information in the bad-card file. This may be immediate in the case of an on-line system or the next banking day in the case of an off-line system.

28. An alternative approach, which has been most evident in respect of some consumer oriented systems, has been to allow the bank to debit the customer's account for the fraudulent transfer, up to a limit of a relatively small amount. The customer bears a risk of loss large enough to encourage him to report the existence of any loss or theft of the plastic card or the compromise of the password, PIN or security procedure, while the bank bears the risk of major loss, thereby encouraging it to strive for a more secure authorization procedure. This approach may be supplemented by a rule that the bank may debit the customer's account for the full amount of fraudulent transfers which are the result of certain actions of the customer. These may include loaning a magnetic stripe card to a third person and telling him the PIN, or writing the PIN on the card or otherwise carrying the two together so that the loss or theft of one results in the loss or theft of both.

29. A third means of assigning the loss in a large number of cases is to place on the bank or on the customer the burden of proving how the fraud took place since in many cases the party who carries the burden of proof will lose. It is particularly difficult to prove that a fraud committed by a third party who has not been apprehended was caused by such actions of the customer as leaving a password in a desk drawer or writing the PIN on the plastic card. It would normally be even more difficult for a customer to show that a bank had designed an inadequate security system or had failed to follow its own authorization and security procedures.

30. Insurance can also be used to shift fraud loss from both bank and customer. However, large or repeated losses are soon reflected in higher premiums.

## B. Errors

### 1. General sources of errors using computers

31. At the time computers were first widely used in some countries for commercial purposes, the experience with the large number of errors encountered was discouraging for the firms that owned the computers and upsetting to their customers. Not only were there large numbers of errors, but it seemed difficult for the firms to correct many of them. However, the early bad error experience of many firms in the use of computers lay in part

in the quality control of the hardware itself and in the inexperience in designing software. These are no longer the source of constant frustration they once were; the hardware is highly reliable and software, while still a problem, is of a much better quality than before. The errors which occur as a result of hardware or software failure are a minute proportion of the total number of transactions.

32. The early bad error experience also lay in the inadequate procedures adopted by many firms in relation to their newly acquired computer systems. In order to gain the volume of transactions necessary to support a main-frame installation, a central data processing center was often established which was organizationally and physically separated from the operating departments which received, generated and used the data. The data processing center was often in a separate building, and in the case of organizations with branches in different cities, it would by necessity be in a different city from many of those branches. The personnel in the operating departments too often did not understand the needs of the data processing department for presentation of data in a consistent format; the data processing department became the province of specialists who too often did not understand the operations and needs of the firm; procedures for eliminating and resolving errors did not always command the same level of support as did the installation of the new equipment; and it was often difficult for customers, suppliers and employees alike to locate the person with authority to rectify problems which had arisen.

33. Although these problems are far from eliminated, it can be said with some confidence that errors arising out of the separation of the data processing department from the operating sectors of the firm and arising out of inadequate internal procedures in general are no longer the source of concern they once were. Operating personnel are more familiar with the procedures required to function with computers and data processing personnel have learned better how to shape the technological needs and possibilities of computers to the requirements of the commercial or administrative activities within which they operate.

34. Equally important, especially in the banking context, has been the decentralization of data in-put to the computer facilities. It is now common in many parts of the world for terminals to be located throughout the operating departments. Tellers dealing with banking customers over the counter can enter deposits and withdrawals directly into the computer, as can operating personnel who receive funds transfer instructions and other banking instructions through the mail, over the telephone or by other means.

35. The decentralization of data in-put in the bank has reduced the likelihood of error in several ways. By entering the data in the operating departments responsible for the transactions, the personnel entering the data are responsible for the entire transaction. They may feel a greater sense of responsibility for the accuracy of the data; they get a response from the computer immediately and know if the transaction was accepted; they are more apt to understand the context in which the data was created, thereby permitting them to recognize ambiguities and to resolve those ambiguities promptly and correctly; and the data need be entered only once in the bank's records, rather than two or more times as sometimes occurred with centralized data processing or with paper-based systems.

36. The introduction of customer-activated terminals with the capacity of ordering routine funds transfers further reduces the likelihood of bank error since the funds transfer instruction would normally be processed automatically without intervention of the bank's personnel. Errors are less likely to occur in a fully automatic electronic funds transfer system than in a semi-automatic system or in a paper-based system. However, the errors that do occur may be more serious because of the extremely large number of transactions processed by computer. Furthermore, there is a constant fear of massive failure out of all proportion to prior experience.

2. Current sources of errors peculiar to electronic funds transfers

(a) Non-standardization of messages

37. Because there is as yet no universally recognized standard format for electronic funds transfer instructions, the possibility of error in composition of the message by the sender and comprehension by the receiver is increased. Moreover, if the message fields in two computer-to-computer funds transfer networks are not fully compatible allowing for automatic conversion from one message format to the other by interface software, a funds transfer instruction received from one network will have to be fully or partially re-keyed to be sent through the second network.

(b) Re-creation of messages

38. Re-keying a transfer message creates the possibility of error. This possibility of error is to some degree unavoidable in all electronic funds transfers. In contrast to paper-based funds transfers where the original paper form filled in by the customer can usually be forwarded through the banking system precluding the possibility that the payment instruction will be altered except by fraud, an electronic funds transfer message is re-created at each processing point. Payment instructions given to a bank in paper form are transformed into electronic messages which may again be reproduced on paper at receipt. Telex transfers through a correspondent bank require the correspondent bank to pass on a new message with a somewhat different data content. Messages sent over packet-switching networks are broken into segments of a uniform length which are sent by separate circuits and reassembled at the destination. Transfer instructions submitted on magnetic tapes to an automated clearing-house are sorted and recorded on new magnetic tapes before being sent to the receiving bank.

39. Each of these processes introduces the possibility of an inadvertent change in the content of the payment instruction through human error, an incorrect computer program or a breakdown or defect in the equipment. However, these errors can be detected before they pass through the system if the necessary controls are designed into the system as well as into the operations of each bank and if those controls are rigorously applied.

(c) Non-standardized procedures

40. International funds transfers, whether electronic or paper, are more difficult for banks to handle without error than are domestic transfers because of the lack of international agreement on appropriate procedures. Each transfer message must, therefore, be read carefully to be sure as to the procedure being used by the sending bank. That message may be unclear, especially when it is composed in unstructured cable language.

41. This confusion may be compounded when the local banking practices in the receiving country are different from those in the sending country. In particular, expectations as to the time within which funds will be made available to the transferee bank and to the transferee may turn out to be incorrect because of a local practice that a correspondent bank may withhold settlement for several days, or that remittance will be made to remote locations by mail or by cheque, even though the international funds transfer instruction requested the highest priority be given to the transfer.

(d) Computer failure and software error

42. One source of errors in electronic funds transfers which does not exist in paper-based transfers is the electronic equipment itself. This includes the computer hardware of the banks, telecommunications carriers and clearing houses or other switches and the software to make them operate. Although errors from these sources are comparatively few compared to those experienced only a few years ago, they are particularly serious. An error which arises out of a mistake in keying a funds transfer instruction into the system affects only that one message. However, a defect in the computer hardware or software may treat an entire series of instructions incorrectly. Moreover, the very nature of the problem in the hardware or software may cause the error to by-pass the validity checks which are built into most computer programs. Most importantly from a legal point of view, errors arising out of defects in the computer hardware or software itself raise difficult questions as to the responsibility for the losses which result.

3. Conceivable methods to prevent errors from occurring

43. Fortunately, most of the actions necessary to reduce the number of errors occurring in electronic funds transfers can be taken by each bank individually. However, some actions can be taken only by the banking community as a whole. In particular, standardized message formats and banking procedures should be established for both domestic and international funds transfers. In some respects agreement at the international level may be the more important as well as the more difficult. Large amounts are transferred through international wholesale networks, and international consumer electronic funds transfer networks are increasing in importance. Moreover, agreement at the international level should lay a firm basis for agreement at the domestic level.

44. The international banking community is currently engaged in several projects within the Banking Committee (TC 68) of the International Standards Organization (ISO) which should lead to generally accepted formats for the most commonly used message types in international funds transfers. ISO Draft International Standard (DIS) 7982, Part 1 contains vocabulary and data elements used in describing, processing and formatting funds transfer instructions. ISO/DIS 7746 provides standard telex formats for inter-bank funds transfer instructions. These standard formats, based upon S.W.I.F.T. message formats, are intended (1) to eliminate misinterpretation by the receiving bank of the sending bank's instruction and (2) to provide a basis from which can be developed systems for the automatic handling of telex funds transfer instructions. Other work of ISO TC 68 on such matters as test keys, technical characteristics of magnetic stripe cards and interchange message specifications for debit and credit cards will also contribute to more efficient, error-free and fraud-free electronic funds transfers.

45. The eventual adoption by ISO of standard formats for telex funds transfer instructions which are in harmony with the S.W.I.F.T. message formats and agreement on vocabulary to be used in funds transfer instructions and their adoption and use throughout the world for both domestic and international funds transfers would reduce the likelihood of errors arising out of the needs to re-key funds transfer instructions. A standard telex format with numeric field tags as well as field descriptors will permit the receiving bank to key the instruction into its computer system for entry into the records of the bank and for re-transmission, if necessary, with no necessity for interpretation of the instruction. This will be of particular value when the sending and receiving banks are from different language areas.

46. It can also be hoped and expected that the international banking community through appropriate institutions will over time be able to agree upon the procedures to be followed by a receiving bank, especially when it is not the transferee bank. It must be recognized, however, that when the receiving bank must re-transmit the funds transfer instruction through the domestic funds transfer system, agreement on the actions it should take would require a large degree of harmonization of the technical means by which funds transfers are processed domestically in different countries as well as the attendant banking laws and procedures. As an interim step, a clearer delineation of the actions which are taken by receiving banks in different countries in standard situations and the time required for these various actions might lay the basis for future harmonization efforts.

## C. Need for customers to verify status of accounts

### 1. Statements of account activity

47. In spite of the most rigorous efforts on the part of all concerned, a certain number of improper entries will be made to the accounts. Once these entries have passed the various controls instituted by the bank to eliminate errors and fraud, they can in most cases be discovered and rectified only by the complaint of the customer. In order for the customer to discover any errors in his account, he must have a means of reconciling the records of the bank with his own record of transactions in that account.

48. There have been two traditional means of furnishing the customer with a statement of account activity. In some countries, perhaps in particular those countries in which credit transfers have been the normal means of inter-bank funds transfer for commercial and consumer purposes alike, a notice is sent by the bank whenever a debit or credit entry is made to the account. The notice can, and often does, indicate the opening balance, the debit and credit entries made that day and the closing balance. A quarterly or yearly statement may also be sent to reflect interest debited or credited to the account and to state officially the bank's record of the account balance. In other countries, a statement of account activity is sent periodically to the account owner. Statements on ordinary accounts may be monthly, quarterly or yearly, while statements on active commercial accounts may be weekly or even daily. Although a daily statement on an active account may appear to be the same as a daily notice to the customer of an active account of debits or credits to the account, it implements a different policy.

49. Where the account is inactive, the customer may receive no statement for a long period of time. In a country in which notices are sent to the customer each time there is a debit or credit to the account, this would indicate that no action had occurred during that period. In a country in which statements of account activity are normally sent on a periodic basis, the bank and the customer may agree that no statement is required because of the infrequency of expected transactions or because the customer wishes to keep the account secret. However, this is a dangerous practice since it leaves open the possiblity that fraudulent or mistaken entries to the account may not be discovered for long periods of time.

50. The advent of customer-activated terminals changes somewhat the need for statements of account activity, whether the statement is furnished periodically or as a notice of debit or credit to the account. If the customer can access the bank's record of his account, and especially if the customer has the facility of producing a hard copy of that record, there may be no need for the bank to go to the expense of mailing statements to the customer. At the present time some commercial customers of many large banks can access their accounts in this manner, and this facility is being actively promoted by banks serving multinational corporations as part of a cash management programme. It is also available in some home banking experiments, but automated teller machines which permit balance inquiry may not permit inquiry as to account activity.

## 2. Customer's examination of the statement

51. There are several arguments for holding that a customer should examine the statement sent by the bank to find fraudulent entries, errors or other discrepancies. The statement, especially a periodic statement, may be seen as an offer to settle the account between the bank and its customer on the basis of the statement, a form of settlement which is known in various legal systems under different doctrinal names. The recipient of the statement must reply within a specific period of time or, in some countries, it is accepted as the correct statement of the account at that point of time, while in others the burden of proof of showing whether it is correct or not shifts from the bank to the customer.

52. The policy supporting this result is directly applicable to a transaction account in a bank. It is useful for the parties to agree periodically on the status of their mutual relations so that at the end of an extended period of time it is not necessary to retrace each entry to the account long after the details have been forgotten and the records may no longer exist. Furthermore, an incorrect entry to one account, whether caused by error or fraud, is often mirrored by an incorrect entry to another account. Delay in notifying the bank of an incorrect entry may reduce the possibility that the bank can correct the transaction or otherwise reduce the loss.

53. In some countries the customer is said to have no duty to examine the statement of account activity and may raise an objection to an incorrect entry at any time until the period under the statute of limitations or prescription has passed. This rule is more protective of the customer and it may be particularly justified in the case of individuals who are either new to the banking system, and therefore are unaware of the need to reconcile their statements or are not able to do so, or in the case of individuals who travel a great deal or live in a distant place and may have more difficulty in receiving the statement promptly. However, even in these jurisdictions it may be contributory negligence if a customer does not examine the statement and object to incorrect entries.

54. It should be recognized, nevertheless, that whatever the rule may be, an improper entry to an account which has passed through the controls of the bank will often be discovered only if the customer reconciles the statement of account activity received from the bank and notifies the bank of the improper entry. This is particularly relevant when cheques are truncated at the bank of deposit and the essential funds transfer data are electronically processed because this practice reduces the likelihood that the transferor bank (drawee bank) will detect a forged signature of the transferor (drawer). The practical difference in the rules lies primarily in the fact that the customer has a shorter period of time within which to notify the bank of the improper entry when the customer is said to have a duty to examine the account than when the customer is said not to have such a duty.

### 3. Duty of a bank to correct entries

55. It is evident that a bank must correct improper entries in the account promptly after being notified of them by the customer, unless there is a legitimate question whether the entry is improper. Detailed rules governing error correction by banks in respect of consumer electronic funds transfers have been adopted by some countries and proposed in others. 1/ The need or desirability of such rules depends on the experience in each country.

---

1/ The right of a bank to correct entries to a customer's account when the error was in favour of the customer is considered in the Chapter on Finality of Honour.

D. Responsibility of an originating bank to its customer for errors or fraud made in an interbank transfer; a network liability approach

56. As used in this discussion, the originating bank is the bank which receives the funds transfer instruction from its customer and transmits it through appropriate channels to the destination bank. In a debit transfer the originating bank is the transferee bank (or depository bank) while in a credit transfer the originating bank is the transferor bank. The originating party is the party who submits the funds transfer instruction to the originating bank. In respect of the issue discussed in this section, there seems to be no particular difference in the law governing paper-based transfers between the transferee bank as the originating bank in a debit transfer and the transferor bank as the originating bank in a credit transfer.

57. The fundamental problem is that associated with any field of economic activity in which a customer contracts with one firm to achieve a result which requires the participation of one or more other firms. The first firm may be held responsible only for its own performance, including the choice of appropriate collaborators, or it may be held responsible to the customer for the performance of all parties necessary to achieve the result contracted for i.e. a transaction liability approach. The closest analogy to the funds transfer situation is that of the carriage of goods by common carrier where the carriage of the goods from origin to destination may require the participation of freight forwarders and terminal operators as well as several carriers of the same or of different types.

58. In favour of transaction liability: Although the originating party designates the general type of funds transfer and the destination bank, with few exceptions, neither the means of communication between the banks nor the intermediary banks are designated. The choice of a proper channel is left to the discretion of the bank. In a highly automated bank this choice may be exercised by a computer according to programmed criteria. Where alternative means of communication or intermediary banks are available, the bank must use reasonable care in the selection of appropriate means.

59. If the funds transfer is not made correctly, it is often difficult to determine where, how and why the error occurred. Each bank, clearing-house, switch and telecommunications carrier has an interest in claiming that the problem did not occur with it. The customer, being outside the system and having no continuing relationships except with his own bank, may find it unusually difficult to investigate and determine who appears to be at fault. If it appears that the party at fault can be sued only in a distant part of the country or in a foreign country, the originating party faces additional difficulties and expense to pursue his claim. However, if the originating bank has accepted or is deemed by the applicable law to have accepted responsibility for the successful completion of the funds transfer, subject to the loss not having occurred for specified exonerating reasons, it would be in a better position to seek reimbursement from the bank or other entity at fault. Under this approach, the originating bank would suffer the loss rather than the originating party if it could not be determined how the loss causing

event occurred. The increase in cost to the banking system as a whole not taking into account any increase or decrease in litigation expenses would be the amount customers had previously been unable to recover because of an inability to prove where or how the error had occurred.

60. In the context of debit and credit cards issued by a bank, these same considerations have led to the opposite result, i.e. to acceptance of the destination bank (often referred to as the card issuing bank in this context) as the sole bank responsible to the customer for any improper debits to his account arising out of the use of the card. If an error or fraud has occurred in connection with the use of the card or the forwarding of the funds transfer instruction for which the customer cannot be charged, the banks in the card network distribute the loss between themselves according to the terms of the network agreement.

## E. Permissibility of disclaimer of liability

61. Disclaimer provisions are found in contracts between the originating bank and its customer and between the banks, clearing-houses, operators of switches, telecommunications carriers and other parties who may participate in the funds transfer. A disclaimer provision may provide that the disclaiming party is not to be held liable for loss caused by third persons, for loss caused by some or all of the disclaiming party's own acts or failures or for certain types of losses, and especially for indirect damages.

62. The extent to which disclaimer provisions in contracts governing electronic funds transfers will be enforced depends in part on the general attitude of the legal system towards such clauses and in part on the extent to which the law governing funds transfers is regarded as mandatory or non-mandatory. It could be expected that disclaimer provisions directly affecting rights and obligations in respect of a negotiable instrument would not be enforced, whereas provisions affecting its collection or affecting electronic funds transfers, neither of which are covered by comprehensive statutes in most countries, might more likely be enforced. Where a statute has been enacted to protect consumer rights in electronic funds transfers, as in the United States, those rights can be modified to only a limited extent by contractual provisions.

63. The contractual disclaimers in contracts between the banks, between the banks and other entities in the funds transfer process, and between banks and their suppliers of computers and software have no formal effect on the relations between a bank and its customers. The customer as originating party may be able to present his claim to the entity whose actions or non-actions caused the loss without regard to disclaimer provisions in contracts to which he was not a party.

1. Technical failure of computer hardware or software

64. Many bank-customer contracts provide expressly or by implication that the bank is exonerated from liability for failure to carry out a funds transfer instruction in the proper manner if it can show technical failure of computer hardware or software. 2/ However, exoneration on these grounds should be carefully limited.

65. Although computers have become considerably more reliable than in the past, computer downtime is a regular occurrence. Banks which use computers for funds transfer and other purposes should have, and normally do have, sufficient redundancy of equipment available either on their own premises or at another firm (e.g. supplier of computer equipment, computer service bureau, another bank or other firm with compatible equipment) to operate during the period their own computers are out of service, although perhaps with some impairment of service. Therefore, computer downtime of an expectable level which should be compensated by redundant capacity should not be readily accepted as a justification for failure to carry out a funds transfer instruction within the otherwise applicable time-limits. On the other hand, some delay may have to be tolerated. Furthermore, computer failure beyond an expectable level, especially if associated with a general disaster or loss of electricity in the area where the bank is located or if associated with a major disaster to the bank, such as a fire, may justify exoneration of the bank.

66. Banks which do not have available sufficient redundant computer capacity should retain the capacity to receive and dispatch funds transfer instructions by other appropriate means.

67. There would be no particular legal difficulties in denying exoneration if a failure to carry out a funds transfer instruction was caused by defective software designed by personnel of the bank. The defective software would seem to be merely the means by which the bank failed in its obligations. The answer would be the same even if the source of the problem was defective or inappropriate software purchased from an outside supplier. In general, neither a bank nor any other business should as a matter of course be exempt from liability because equipment or software it uses in its business is inadequate for the task at hand.

---

2/ The related problems as to whether a bank should be exonerated for failure occuring while the instruction was transitting the telecommunications carrier which is itself immune from liability or while transitting a clearing-house or switch owned by or operated on behalf of a group of banks are treated in paragraphs 68 to 73 and 78 to 81.

2. Data communications service

68. Most inter-bank and many intra-bank electronic funds transfers must use the services of a data communications service. Traditionally the telecommunications carriers have often been free of most liability for harm as a result of the delay or non-delivery of a message or for any change in the content of the message.

69. The argument in support of exemption from liability that the telecommunications carrier could not foresee the consequences of a late or non-delivered message or of a change in its content because it did not know the content has not always been satisfactory in respect of telegraphic or telex service where the customer handed a message to the carrier to be transmitted. In many cases the personnel of the carrier fully understand the significance of the message being sent. In any case, when the damages were unforeseeable, at most the types or amount of damages might have been limited, but this did not justify complete exemption from liability.

70. Computer-to-computer telecommunications over a common carrier would seem on their face to be a prime example of a case in which the carrier has no idea of the content of the message, especially when the message is encrypted. Once the integrated services digital networks (ISDN) are installed, the carrier may not even know whether it is carrying data, written messages, voice or pictures; all will be transmitted as a string of digits. However, at the same time, the carriers are no longer limiting themselves to the provision of a basic telecommunications service. As the line between computer services and telecommunications has blurred, the carriers are offering sophisticated enhanced services while the purveyors of computers and office equipment are linking their equipment together into networks. In many cases a bank or other user can receive the same or equivalent service from either a value added network (VAN) or from the telecommunications carrier. Among the services available in many countries which no longer are the exclusive province of the carrier is the ability to switch messages. Therefore, even if the carrier's exemption from liability remains a good public policy in respect of the basic external telecommunication service, the exemption from liability for that basic service should be restricted to those services not available from other sources which do not have the same exemption.

71. In many countries telecommunications services have been provided by the State, often through the same ministry as the postal service. As a result, the telecommunications service has benefitted from the general exemption of the State from liability. Where necessary, the general exemption has been buttressed by a specific regulation protecting the telecommunications service. In countries where the telecommunications service has been provided by private companies, the regulatory structure within which these companies have operated has permitted the limitation of liability in the tariffs filed by them.

72. However, the former monopoly position of the telecommunication carriers may no longer be self-evident and the question has been raised whether the exemption from liability should continue to be sustained. The deregulation of domestic carriers in the United States has already removed the former legal

basis for exemption from liability in that country. It is not as yet clear whether the courts will still sustain clauses inserted in contracts by the carriers purporting to limit liability for their own negligence.

73. Questions of liability are a secondary issue within the broader debate over the future shape of public data communications services. However, as major private users, such as banks, establish private networks in which they control the facilities and take the risk that messages will be late, non-delivered or altered in transmission, the public telecommunications carriers will be under increasing pressure to take an equivalent risk.

### 3. Should an originating bank be exonerated from a delay or non-delivery of a funds transfer instruction after dispatch

74. Since it has not been possible to hold the telecommunications carrier responsible for losses arising out of its failure to deliver a message properly, parties using telecommunications have acted to allocate between themselves the resulting losses. In the context of funds transfers by telegraph or telex, it has been normal for banks to provide in their contracts with their customers that the bank was not responsible for such losses. As a result the customers of the banks have borne the entire risk that the funds transfer message would not be received or that it would be received in an altered condition. The reasonableness of such a contract provision was based upon the inability of the bank to exercise any control over the message once it was handed over to the carrier for dispatch.

75. The reasonableness of the contractual provision is less obvious when the message is sent by the bank on its own telex machine directly to the telex machine at the receiving bank. The carrier furnishes only the circuit and the switch to connect the two machines. The bank sends the message, it can request an answer-back to verify that the proper connection has been made, and it can send a test-key to establish the identity of the sender and verify that key portions of the message have not been altered by error. When there is any doubt whether the message has been received correctly or the message is particularly important, at the cost of a second transmission the sending bank can request the receiving bank to repeat the message in full.

76. All of the possiblities available to verify the receipt and the correct content of a funds transfer instruction sent by telex are also available to the sending bank in a computer-to-computer message. Additional safeguards are available in closed-user networks such as S.W.I.F.T. where all transactions entering the system are validated to ensure that they originate from an authorized terminal, that they meet mandatory format and message-text standards and that they are addressed to a valid S.W.I.F.T. recipient. The messages sent by each bank are assigned an out-put sequential number and the messages received by each bank are assigned an in-put sequential number, reducing to a minimum the possibility that a message will be lost. Store-and-forward capability reduces the likelihood that a message cannot be delivered and undeliverable message reports assure the sending bank that any messages which could not be delivered were accounted for. Alternate routings are provided in case one of the switching centers is out of commission and member banks are instructed on how to access the S.W.I.F.T. network over the public switched network in case of failure of the regional processor.

77. Not all of the safety measures taken in a closed-user network such as S.W.I.F.T. are available to a bank operating over a public switched network. Nevertheless, procedures can be followed which reduce to a minimum the possiblity that a failure in the communication net will go undetected and uncorrected by the sending bank. The availability of these techniques to avoid errors arising during transmission of the electronic funds transfer instruction raise serious questions as to whether banks should be free to avoid liability for such errors, even if they cannot seek reimbursement from the carrier.

F. Malfunctioning in an electronic clearing-house or in a switch owned by or operated for a group of banks; loss sharing by participating banks

78. A clearing-house is an integral part of the funds transfer system. It may be operated by the central bank, another large bank or the banking association. Alternatively, the clearing-house may be organized by a group of banks. In some countries on-line electronic funds transfer networks have been established in which the message switch without a net settlement function is operated for the participating banks by a company which is neither a bank, clearing-house nor a telecommunications carrier. The company may be a computer service bureau, value added network or the like.

79. In many cases the clearing-house or switch provides in its regulations or by contract with the participating banks that it has no liability or only limited liability for errors or fraud which occur at the clearing-house. If the clearing-house is operated by the central bank, the liability of the clearing-house or central bank may be limited or excluded by statute, by regulation or by general doctrines of law applicable to agencies or instrumentalities of the State. However, since the clearing-house is acting for the banks, exemption from liability may not pose the same level of concern as it does in respect of telecommunications carriers.

80. Nevertheless, it is significant that a clearing-house is an integral part of the funds transfer system. It cannot be argued that the banking system as a whole should not be held responsible to its customers for the failures of a clearing-house, as it could in the case of a telecommunications carrier. It seems evident that the originating party should in principle have an effective means of pursuing any claim arising out of such a failure.

81. At the same time, the collective nature of a clearing-house or switch for banking transactions may call for a sharing of the resulting losses among the participating banks. There are a number of ways in which a sharing of losses can be arranged, including insurance, constituting a compensation fund and levy upon all of the other participating banks. The losses which may be attributed to a clearing-house or a switch, and therefore subject to sharing, might include losses suffered by a bank as a result of following the procedures outlined for transfers through the clearing-house or switch. In particular, it may be appropriate to share losses which are attributable to a weakness in the security system, including the procedures and the algorithm for enciphering the funds transfer instructions.

## G. Improper handling of transfer instructions

### 1. Wrongful dishonour of instructions by a transferor bank and damages to the transferor

82. The transferor bank is responsible to the transferor for damages suffered as a result of the bank's wrongful dishonour of a proper funds transfer instruction. A bank which dishonours a credit transfer instruction should inform the transferor promptly of that fact and the reasons for so doing. The transferor's claim for any damages resulting from improper dishonour would be evaluated and settled as would any other claim arising out of delay in effecting a funds transfer. Wrongful dishonour of a debit transfer instruction may have more serious consequences. When the transferee of a debit transfer instruction is notified that the instruction has been dishonoured, whether or not a reason is given for the dishonour, doubts as to the solvency and the integrity of the transferor naturally arise. If the dishonour was wrongful, the transferor bank (e.g. drawee of a cheque or bill of exchange) should also be responsible for the damages which were caused to the transferor in that connection.

### 2. Inaction on debit instructions by the transferor bank within the required time-limits

#### (a) General rules for negotiable instruments

83. If the transferor bank does not act within the required time to honour or dishonour a debit transfer instruction or to give notice of its dishonour, the transferee has a claim against the transferor bank.

84. Except in France and other countries which follow the doctrine that a negotiable instrument transfers to the holder ownership of the fund (provision), i.e. the right in the account up to the amount of the instrument, the standard doctrine in respect of cheques and bills of exchange is that the instrument is not such an assignment and that the transferee (payee or other holder) has no right on the instrument against the transferor bank (drawee) until the instrument has been honoured. However, once the instrument has been presented to the transferor bank for honour, the bank may have a duty to the transferee or to the transferee bank to act within certain time-limits either to honour or to dishonour the instrument. If the instrument is dishonoured, the transferor bank owes a duty to the transferee to give a prompt notice of the dishonour. The party to whom the notice of the dishonour may or must be given varies in different countries and in some countries the notice must be given by formal protest.

85. These rules from the law governing paper-based negotiable instruments and their collection should be generally applicable to debit transfers in electronic form. However, since these rules usually appear in statutes governing negotiable instruments or in the law or agreements governing their collection, it may be necessary to extend them to electronic debit transfers.

(b) Delay in honouring debit transfer instruction

86. If the transferor bank honours the debit transfer instruction, but does so later than it should have under the applicable rules, the consequences of its delay depend on the means by which settlement was made. If the transferor bank provisionally settled for the instruction when it was presented, for example, by net settlement through a clearing-house, the delay in honouring would have no practical consequences. If settlement for the instruction was delayed until the instruction was honoured, the presenting bank would be denied use of its funds for the period of time of the delay. The transferee in turn may not have been given credit for the transfer until the transferee bank received credit. The delay may, therefore, lay the basis for a claim of damages such as for loss of interest or, in an international transfer, for exchange losses.

(c) Delay in dishonouring debit transfer instruction

87. The delay in dishonouring a debit transfer instruction by the transferor bank sometimes arises because the transferor is on the edge of insolvency. In some cases, when there is not sufficient funds in the transferor's account to honour the instruction, the transferor bank may wish to give the transferor time to replenish the account so as to be able to cover the outstanding instruction. In other cases the bank may, whenever possible, wish time to decide whether to set off against the transferor's account other obligations due it from the transferor before it honours the funds transfer instruction. In either case, the instruction may subsequently be dishonoured.

88. In such a case, the debit transfer instruction may be deemed to be honoured or the transferee may be allowed to recover for the delay. However, the transferee may find it difficult to prove the amount of its loss in these circumstances. It would be possible to overcome this problem by placing on the transferor bank, which was in delay, the burden of proof of showing that the transferee had suffered no loss from the delay. Another way to achieve the same result would be to permit the transferee to recover the face amount of the instruction from the transferor bank and to assign to the bank the transferee's rights in the insolvency proceedings of the transferor. 3/

H. Recoverable losses

89. An improperly executed transfer can lead to a loss of part or all of the principal amount transferred, as well as to consequential losses. In the context of a funds transfer, consequential losses can arise out of loss of interest, changes in exchange rates and indirect losses arising out of lost business opportunities and the like.

---

3/ The periods of time within which the transferor bank should honour a debit transfer instruction or should give a notice of the dishonour are discussed in the Chapter on Agreements to Transfer Funds and Funds Transfer Instructions, A/CN.9/250/Add.3, paras. 77 and 78.

1. Loss of principal

90. When an electronic funds transfer is credited to the wrong account, credited to the correct account for an excessive amount or processed twice, the transferor or the transferor bank risks losing the principal amount of the incorrect transfer. In most cases, the error can be rectified by a debit to the account of the incorrect transferee with a corresponding credit to the account of either the transferor (in which case the transfer has been reversed) or to the correct transferee (in which case the transfer has been made correctly). 4/

91. If the incorrect transferee withdraws and uses the funds, whether or not he knew of the error, and subsequently is unable to restore the amount used, the loss of principal must be allocated between the transferor and the bank or banks at which the error occurred. Similarly, if a transfer has been made fraudulently, the resulting loss of principal must be allocated between the transferor, whose account has been debited, and the bank or banks where the fraud may have occurred. In cases of loss of principal there is seldom any argument over the amount of loss which is to be allocated. The argument goes, rather, to determine which party should bear the burden of the loss, a subject covered by the general rules on liability discussed above.

2. Loss of interest

92. The one form of consequential damages which has generally been admitted in the law has been interest when payment of a sum due was late. Interest claims for late funds tranfers by commercial customers of banks are now a frequent occurrence. In part this is because interest rates are high and the amount of interest which can be earned in even one day is measureable and may be worth claiming. In part it is because of the funds transfer possibilities made available to corporate treasurers by the new electronic funds transfer techniques. When commercial payments are made by slow paper-based credit transfer methods, a transferor cannot withhold his funds transfer instructions to the last moment before payment is due. It is understood that the time between the debit to the transferor's account and the credit to the transferee's account might be sizeable and somewhat unpredictable. However, now that some banks advertise their ability to transfer funds instantaneously, many commercial customers attempt to retain their cash until the last possible moment before issuing funds transfer instructions. Cash management techniques have made public and corporate treasurers throughout the world conscious of the interest earning potential of their cash balances.

93. Sometimes it is the transferee rather than the transferor who should have the right to claim interest. In the typical electronic credit transfer the transferor's account is debited before or at the time the funds transfer

---

4/ The right of the bank to debit the incorrect transferee's account without his prior consent is discussed in the Chapter on Finality of Honour.

is sent. If the transfer is delayed, it is the transferee who is denied the use of the funds, not the transferor. Nevertheless, the transferee is currently understood to have no right against any bank, except perhaps his own, to claim interest because of delay in completing the funds transfer. 5/ If indeed the payment is late under the underlying agreement, the transferee's claim for interest because of late payment would be against the transferor. The transferor in turn may have a right of reimbursement from his bank or from the bank at fault. The problem, however, is how to determine the exact period of time within which a funds transfer should take place. There are few agreed rules on the matter.

94. With regard to adjusting interest charges between banks, there are several sets of rules governing the allocation of interest when the delay in transfer of the funds was due to the fault of one party or the other. Many of the rules governing the reimbursement of lost interest allow recovery only if the claim is for more than a specified amount. An interesting feature of the most prominent set of rules in use in the United States for compensation between banks when the claim is the result of an inter-bank funds transfer error is that the bank which receives money by mistake from another bank is required to pay to the bank which sent the money by mistake interest at the prevailing rate, less a service charge to the receiving bank. The rationale which lies behind this provision is that a bank which receives money will have the benefit of its use.

95. The existing rules, however, are limited in their application to the bilateral relation between any two banks or, in the case of some interbank telecommunications systems or clearing-houses, such as S.W.I.F.T. or CHIPS, to some losses caused by that system. They specifically do not apply to losses caused by or to third parties.

### 3. Exchange loss

96. With exchange rates fluctuating daily, customer claims for reimbursement of exchange losses arising out of late payments have become a more frequent occurrence. By the nature of the loss, claims for losses occasioned by an adverse movement of the exchange rates during the period of a late transfer will normally be made only by transferors of large sums. However, in the case of a devaluation by a significant percentage, customer claims arising out of international consumer transactions or consumer transfers should also be expected. The difficulties of establishing the appropriate period of time within which the transfer should have been made apply as much to losses occasioned by adverse movements of exchange rates as to loss of interest.

---

5/ By analogy to the law governing the carriage of goods, where the consignee of the goods has a right to claim for the damage even though the contracting parties are the shipper and the carrier, consideration might be given to providing the transferee a convenient means of claiming lost interest in appropriate cases.

97. However, a claim for loss arising out of an adverse movement of the exchange rate will not normally be presented as such. Instead, it will be asserted that the date for conversion from one currency to the other should be the date on which the conversion would have been made if the transfer had taken place properly. Giving the customer the choice between the exchange rate on the date the conversion should have taken place and the exchange rate on the date it did take place is the policy expressed in articles 71 and 72 of the draft Convention on International Bills of Exchange and International Promissory Notes, prepared by a Working Group of the United Nations Commission on International Trade Law, which provide that in case of dishonour of an instrument by non-payment, "the amount to be paid in local currency is to be calculated, at the option of the holder, according to the rate of exchange ruling on the day of presentment or on the date of the actual payment." This option is given to the holder "in order to protect him against any loss he may suffer because of speculation by the party liable." (A/CN.9/213, article 71, commentary, para. 8).

4. Indirect damages

98. The least frequent, but potentially the most serious losses are the indirect damages suffered when a contract is lost, a penalty is incurred or a ship is withdrawn from a charter-party because a required payment was improperly handled. When these events occur, the damages can easily amount to many times the size of the transfer. In most electronic funds credit transfers the party who usually suffers the harm is the transferor who did not fulfill a contractual obligation to pay on a certain date or who missed a business opportunity which required having funds available at a particular place at a particular time. On occasion the harm may be suffered by the transferee who does not have the funds available when needed and who cannot find alternative funds.

99. In some systems the bank is held not to be liable for the indirect damages which it could not foresee at the time it received the funds transfer instruction from the transferor unless the bank deliberately delayed the funds transfer or was grossly negligent. This rule is a direct application of general principles of contract law. However, the limitation on indirect damages to those which are foreseeable is not completely satisfactory in the context of electronic funds transfers. It is particularly difficult for a transferor to give the required information to the proper parties in a legal system which does not recognize network liability. Even if the transferor bank may have had the requisite information to foresee the eventual indirect damages, it would often be the case that the information was not passed on to the intermediary bank or transferee bank at which the negligent actions occur. Neither the S.W.I.F.T. format for a customer transfer nor the ISO draft international standard telex format for a customer transfer (DIS 7746) provides a field for informing the intermediary bank of the possible consequences of a failure to credit the transferee's account by the pay date, although this information could always be added to the instruction by the sending bank. In one recent frequently discussed case, the intermediary bank was negligent in allowing its telex machine to run out of paper without cutting off the machine. It may be of interest that the same negligence which

caused the funds transfer instruction to fail precluded the possibility that the intermediary bank could receive the information which might have made it possible for it to foresee the eventual damages.

100. It is often pointed out that, if banks were to be routinely held liable for indirect damages, the fee charged for funds transfers would need to increase several fold. However, transferors making particularly important transfers might be willing to pay a premium for guaranteed performance by the bank. Therefore, consideration should be given to a new "guaranteed performance" message category in addition to the existing categories. Failure to perform as guaranteed would subject the bank to indirect damages suffered as a result.