THE TELEBANKING CONTRACT IN SWISS LAW*

*Cédric J. Magnin***

---

* Editor's note: This article was translated from the French original in November 2000. Several of this article's Internet sources may be found on World Wide Web servers located in both the United States and Switzerland. Where possible, Uniform Resource Locator (URL) citations point to documents located on servers accessible from the United States. Where site security prohibits site access by Internet users located in the United States (as discussed in Section VI.A.4.b. of this Article) a notation has been made and the source may be obtained from the author.

** Cédric J. Magnin was born on May 3rd, 1973, in Geneva, Switzerland. In 1998, he graduated from the University of Geneva Law School with a J.D. in Swiss law. In 2000, he graduated from Santa Clara University Law School in California with an LL.M. in high-technology law. He speaks French, English, German, Spanish and Portuguese. He is an expert in technology law, particularly in international cybercrime. He is presently a research assistant in Biotechnology Law at the University of Geneva and may be contacted at cedric.magnin@email.com.

I. INTRODUCTION

Telebanking is a means of communicating with one's bank with the aid of a computer connected to the Internet at any hour, day or night, anywhere in the world. It enables a customer to consult their account or transmit banking orders via the Internet. When a customer transmits a banking order via the internet, it is directly stored in the data processing system of the bank and then transmitted to the qualified person in order to carry it out. This method avoids a human intermediary that would normally redirect the orders within the bank to the appropriate person to be carried out.

Telebanking is financially interesting for both the bank and the customer, but it is not risk free. For example, in 1994, two Russians set up a fictitious bank, the European Union Bank Ltd., and stole approximately ten million American dollars. All the funds put under deposit were never found after the closing of the bank by the authorities of Antigua in August 1997.[1]

The first Swiss company to offer a telebanking service was Crédit Suisse (Crédit Suisse Group AG). Other finance companies such as the Post Office and the Union of Swiss Banks (UBS AG) then followed suit. In the next two to three years, the majority of the major financial establishments will propose even more telebanking services at a reduced cost. The low cost of these services is the principal driving force of their development. For example, the use of the data processing department is in itself free, and the underlying contracts (the commission in the event of stock exchange operations and giro banking in the event of payments) are proposed at very competitive prices if they are carried out via the bank's telebanking Internet site.

These competitive prices are possible because of the drastic reduction in costs. Specifically, a central computer has replaced human intermediaries or assignees within the bank.

Statistics show evidence that the electronic banking industry is still growing globally. In March 2001, the largest bank of Switzerland, UBS AG, had 586,000 customers under a telebanking contract, an increase from the last survey in December 2000 which reported 555,000 contracts. Moreover, 23% of all banking orders in Switzerland were placed online, and 13.8% of all stock exchange transactions booked in Switzerland were routed through e-banking transactions.[2]

Moreover, the UBS server experienced 1.5 million logins per month, 30 000 to 40 000 users per day, and 350 to 600 parallel sessions per day.

This trend is likely to continue at an exponential speed because everyone finds telebanking to be in their best interest. First, the banks save costs and gain new customers who are interested in technology, or simply eager to open up an account in a Swiss bank; second, customers pay much less for their banking services, and can place their orders or

---

1. Gambling Magazine, *Money Laundering in Antigua a Risky Business—A Caribbean Bank with Numbered Accounts*, *available at* http://www.gamblingmagazine.com/articles/21/21-144.htm (1999).

2. *See* UBS Switzerland, *E-Channels and Products*, *at* http://193.41.97.55/pdf/ch-ech~1.pdf (citing BlueSky Internet Marketing Inc., E-banking Ratings Survey) (last visited Oct. 4, 2001).

consult their accounts at will, without having to telephone a manager who is absent or busy, or having to place an order at the window of the bank.

Moreover, the current trend is data processing, and particularly the Internet. According to a survey carried out by Nielsen Research Media and Commerce Net (NRM)[3], among the seventy-nine million Americans who have been using the network for longer than sixteen years, more than twenty million say they buy products, and services on the network. On a worldwide scale, the number of Net surfers was approximately 242 millions in January 2000. Thus, there is an increasingly strong trend to move the services on this network, particularly banking services.

However, these new means of communication with banks pose many legal problems. For example, is bank secrecy maintained? Is the network properly protected to make it possible for transactions to be completed without being intercepted? Will a new form of electronic "hold-up" be developed, that creates a new race of criminals, commonly known as "hackers" or "data-processing tapers?" How can we qualify the network? What are the principal obligations of a bank to the customers in this new type of relationship? Is the customer or the bank legally protected from these new problems when the bank does not want to extend a guarantee, and shields itself from responsibility should problems arise? This is precisely what we will try to analyze while studying this new relationship, and the rights and obligations contained in a telebanking contract.

II. DESCRIPTION

A. What is Telebanking?

1. Definition

As its name indicates, telebanking makes it possible to conduct banking operations ("banking") from a distance ("tele"). This concept should etymologically indicate the various ways of conducting banking operations from a distance. For example, by telephone, by mail, by fax or by data processing and data exchange over the Internet, or another data-processing network. These practices have restricted the use of the word "telebanking" to mean primarily banking operations conducted from a distance by means of a computer connected to a data-processing network, the most significant of these being the Internet. Thus, today the word "electronic banking" or "e-banking" is more widely used than "telebanking".

---

3. CommerceNet, *Industry Statistics Worldwide Internet Population*, *at* http://www.commerce.net/research/stats/wwstats.html (2001).

2. History

a. The Eighties

The first experiments with telebanking were conducted in the early 1980s. These experiments used national telematics data-processing networks like the Minitel in France, Compuserve in the United States and the Videotex in Switzerland. Some of the problems plaguing the system were attributed to these networks being slow, incompatible, and not being very user-friendly. Thus, these networks did not accommodate the needs of the standard user during this time period who sought a fast, sure, and financially interesting banking service that would make it possible to conduct banking operations from various countries.

b. 1995: The Birth and Development of the Internet

In 1995, everything changed with the advent of the Internet. As a result, telebanking services became faster, more user-friendly (complete with color and images), and internationally accessible. However, telebanking was still missing one crucial component to complete the evolution of the telebanking system- adequate security.

c. 1998: The Boom of Electronic Trade

It was not until 1998 that electronic trade started to attract a significant number of users. Until that date, only a marginal number of people "dared" to transmit their credit card numbers to a virtual store to make purchases or pay for a service. The increasing confidence of users in the security of the network did not start becoming visible until late 1998. During this period, there was an explosion of "online" credit card purchases during the holiday seasons. However, because these were not significant, it still did not appear that Internet users were ready to use the Internet to conduct significant banking operations.

d. November 1999: Massive Growth of the Offer of Telebanking

Today, we are watching the development of telebanking services at increasingly interesting prices. This is in response to the keen demand. This demand seems to be imminent, due to a combination of various factors. The most significant factor is the awareness, by the increasing number of Net users of the security of the network. Another factor is the unprecedented development of an economic sector, close to that of telebanking: electronic trade. Electronic trade is becoming a habit for most Net users. As a result, there are numerous companies that have specialized in the sale of items or services through the Internet. For

example, in 1998, amazon.com[4] published a quarterly turnover of eighty million American dollars.[5] One year later, during the same period, the turnover was 290 million dollars.[6] In only one year, sales increased by 350%. In the year 2000, sales were predicted to border the billion dollar mark. This growing development of electronic trade for items of nominal value made it possible to compile statistics that reflected a very small proportion of cases of fraud involving credit card numbers when they are transmitted to a protected site. In addition, because credit card companies receive a commission on each transaction, they each have created a special fund which, in the event of fraud, will compensate fraud victims in order to encourage the consumer to communicate his number online.

As a result, potential telebanking customers can feel confident that use of their credit card to buy products, and services on the Internet, through a protected site, does not involve great risk. This contributed to convincing them that this would also be applicable to the banking services offered by telebanking means. In addition, the end of the economic crisis, and the explosion of the financial markets linked telebanking to technology, and Internet transactions. The constant increase in the number of small investors who are potential customers of "online banks" have strongly contributed to the development of telebanking, which appears to have a bright future.

3. The Offer is Available in Switzerland Today

This trend is reflected in Switzerland where there has been a sharp increase in the number of banking services, and Internet telebanking sites that were opened in the spring of 1999. For example, the Post Office opened the site www.yellownet.ch in the Spring of 1999; Crédit Suisse began offering its service www.youtrade.ch in the Summer of 1999; and the Union de Banques Suisses (UBS) started "tradepac" www.ubs.ch\tradepac in Fall of 1999. These three companies already had a functional telebanking service for quite some time, and they have constantly improved over the years. However, these three new Internet

4. *See generally* Amazon.com, *at* http://www.amazon.com (last visited Nov. 29, 2001). Amazon.com is the world's largest virtual shop. It sells books, music, toys and various other new or used items through its auction department.

5. *See* Amazon.com, Inc. Form 10-K405 (Mar. 30, 1998) *available at* www.freeedgar.com. The Form 10-K405 is a report to the United States Securities and Exchange Commission.

6. *See* Amazon.com, Inc. Form 10-K405 (Mar. 5, 1999) *available at* www.freeedgar.com.

sites represent a considerable improvement in tariffs,[7] ease of use[8] and speed. Because of their aggressive marketing operations,[9] these three new Internet sites also show the will of their management to quickly convince a great number of potential customers to use their services. In addition, it should be noted that the banks now make a distinction between the traditional telebanking type service (accessible through the official and global server of the bank[10]), and the specialized telebanking service (equipped with a proper name and without a direct relationship with the bank), which is accessible through a distinct Internet address.[11]

Traditional telebanking makes it possible to inquire about one's account, to make transfers, to place Stock Exchange orders, and to inquire about courses or stock exchange information. Specialized telebanking makes it possible to carry out specific transactions: For example, to buy or sell in the stock exchange, to make transfers, and to apply for loans. It was created partly in reaction to the very competitive American banks which offer these services.[12]

---

7. *See generally* UBS, *Welcome to UBS Financial Services Group*, *at* http://www.ubs.com (last visited Mar. 27, 2000) [hereinafter *Welcome to UBS*].

8. UBS is the first Swiss bank to offer a telebanking service not requiring the prior installation of any software. *See generally id.*

9. They are not bothered to buy full-page adverts in financial magazines and also in popular dailies such as Le Temps, Le Matin, or Tribune de Genève. Bill-posting campaigns in front of the universities like that of Geneva show these companies' intentions of reaching a very wide audience.

10. *See, e.g.*, UBS, *Meinen Enkel aufwachsen sehen*, *at* http://www.ubs.com (last visited Feb. 14, 2001); UBS, *Willkommen be: UBS*, *at* http://ubs.ch (last visited Feb. 14, 2001); La Poste Suisse, *Poste finance lance une nouvelle plate-forme financiere*, *at* http://www.poste.ch. (last visited Feb. 14, 2001).

11. *See, e.g.*, Crédit Suisse, *Welcome to youtrade*, *at* http://www.youtrade.ch. (last visited Feb. 14, 2001); Yellownet, *Yellow Net: Zahlen mit dem Gelben Konto im Internet [Payments via Internet]*, at http://www.yellownet.ch. [Parts of this World Wide Web site may be inaccessible due to site security. Document may be obtained from the author. -Ed.]

12. As an example, the American online broker E*trade enables its customers to buy shares and stock coded for example at the NASDAQ stock market for a token price of $19.95 (except for stock options) per transaction. Datek has a token price of $9.95 per transaction and even offers the latter free of charge to its customers if the order is not executed the minute after it is sent by the customer. Meanwhile, Crédit Suisse continue to receives very high commissions with regards to American companies; about 1.8% with the Federal stamp duties for small amounts. However, with its telebanking service, the commission amount dropped by about 50%, moving to 0.8% if the transaction is made on the Internet. This drop is significant but may not be enough to counter competition from American banks, which, on a transaction of $100,000 carried out at the NASDAQ, still offer an eighty times better value than a Swiss bank.

B. Material Required

The person wishing to use telebanking must fulfill certain prerequisites.

1. Bank Account

Initially, he must have a bank account in the bank that is providing him with this service. Therefore, all the usual checks, such as the identity of economic beneficiary, the origin of the funds, are made in order to prevent the deposit of proceeds from criminal activity.

2. Telebanking Contract

Secondly, he must sign a telebanking contract with his bank which sets out the rights and obligations of the customer, and limits the responsibility of the bank in the event of any loss that is suffered by the customer. This standard contract is available in all the branches of these banks or can be downloaded from the Internet.

3. Provider of Internet Accesses

Third, he must have a contract with an Internet access provider which will allow him to connect to the network either by telephone, cable, electricity or satellite. However, this condition is not necessary if the user does not wish to utilize his banking operations from his residence. Otherwise, he will still be able to use an Internet connection at his place of business or in an Internet cafe.

4. Computer

Fourth, he should have a computer that has a basic configuration, which can be different with each connection. Each bank announces, and sets its own general conditions, and terms. However, Internet telebanking sites are constantly being improved. They require tools that are increasingly more powerful and complex, to guarantee the security and to develop the range of banking services offered. The figures published under the general conditions of the banks at the time the telebanking contract is executed can only have an indicative value and must constantly be modified.

Currently, the Telebanking user of UBS., Crédit Suisse or the Post Office must have, at minimum, the following:

- a Pentium processor13 (for a PC)14 or Power PC (for a Macintosh15 computer);

13. It is the brain of the computer, which controls and runs all its operations.

- 10 Mb16 of space on the hard disk17 in order to back up the encoding software. However, this is no longer necessary for the last version of telebanking offered by UBS, which is the first Swiss bank to offer an access to telebanking services without preliminary software;

- 32 Mb of RAM18 to be able to correctly view the Internet pages of the telebanking site;

- A current operating system[19] (Windows 95\98\2000\Me\XP, Windows NT 4.0 service pack 4, Mac OS 8.x, Unix or Linux); and

- A modem[20] with the fastest possible speed so that communication with the Internet site of the bank is quick, and Internet navigation software as recent as possible to be able to follow the trend of the telebanking sites (Netscape 4.0 or superior, Microsoft Internet Explorer 4.0 or superior).

C. Security

1. Coded Transmission Between the Bank and its Customer

Swiss banks have a particular obligation to respect bank secrecy that the majority of the banks in foreign countries do not have. However, bank secrecy or not, information transmitted between a bank and its customer is highly personal and any bank, whether it is Swiss or not, must seek powerful software allowing it to cipher information passing through the

---

14. Abbreviation of "Personal Computer": the single link between these computers is their inter-compatibility regardless of their label and account for about 90% of the computer market.

15. These computers are not compatible with PCs except for some specific applications having special "pathways." They account for about 10% of the computer market.

16. Abbreviation of "Mega Bytes," computer unit equivalent to one million 'bytes', each 'byte' being itself made up of a combination of eight figures composed by zero and by one. A minimum space enabling to safeguard eighty million (=8*10*1.000.000) figures in the hard drive of the computer.

17. Name given to a computer devise used to store data in the computer.

18. Abbreviation of Random Access Memory.

19. Computer program running and presenting the software used by the computer in a specific way (e.g. Windows has a very friendly presentation in the form of windows, which is not the case for Unix, which is more appropriate for professionals).

20. Common name given to the apparatus that transforms the data which the user wants to transmit on the internet network in a format that enables it to travels on lines or on any other medium (modulator) and retransform data its receives in a format that is readable by the computer (demodulator).

network and to ensure its customers of the confidentiality of the information exchanged.

a. Encoding Software to be Installed on the Computer of the User

The first experiments in telebanking required the installation of special software to cipher the data on the user's computer.[21] However, this solution is not very practical because it does not make it possible to carry out banking transactions on any other computer other than the one on which the software is installed. This is why banks are all replacing this software with an autonomous system of coding.

b. An Autonomous Encoding System: SSL

UBS was the first Swiss bank to propose to its customers a system of autonomous coding not requiring the installation of software on the computer of the user for it to function.[22] The majority of the American banks offering the service of telebanking adopted it for a considerable time, and it is about to become the model for computer security. This system of coding, called Secure Socket Layer (SSL), is a public protocol which ciphers data passing between the Internet navigator used by the customer (Netscape, Explorer), and the server of the bank. The banks maintain[23] that the "coding used currently enjoys a very high level of security", and "Protection obtained is an obstacle to professional hackers". "Generally, the Internet Banking system is safer than the usual procedures of sending payments, and orders through the post office". "It is a coding with 128 bytes (IDEA\RC4) or 168 bytes (3DES)."[24] SSL is so powerful that the American authorities require government authorization for its export. This authorization is only granted to specific companies. Exportation of SSL, without authorization from the proper authorities, is considered, by the United States, to be exportation of an illicit weapon carrying a punishment of two years of imprisonment.[25] Indeed, by using SSL in a communication system, it enables these types of criminals to communicate among themselves by using the code, while it provides some

21. This is still the case with Crédit Suisse's and the Post office's telebanking site.

22. *See generally Welcome to UBS, supra* note 7.

23. Based on an interview realized in October 1999 with UBS and Crédit Suisse legal departments.

24. UBS, *Why UBS e-banking classic is so secure, at* http://www.ubs.com/e/ebanking/classic/security_info.html (2001) [hereinafter *Why UBS e-banking classic is so secure*].

25. This American law, which is not applied with flexibility, has been used to convict people.

certainty, and assurance the police could not intercept their conversations. This is precisely why the United States tries to ensure that terrorists or other criminals cannot use SSL for dubious purposes.

c. Financial Certificates

A "Financial Certificate" is a certificate which grants accreditation to the server.[26] The Financial Certificate was established by an accreditation and certification office. The Financial Certificate certifies that the server to which the user is connected is authorized to use a system of coding (SSL or other), and the Financial Certificate attests the level of security employed by this system (40, 56, 128 or 168 bytes for principal coding which is currently used). The goal of the Financial Certificate is to prove to the user that he is actually communicating with his bank, and not with a pirate site. Additionally, each Financial Certificate has a "fingerprint" which is unique to it, and which can be checked by the user each time he is connected. Upon getting information from his bank or from the office of accreditation and certification, each user will know the official fingerprint of the telebanking site. This will enable the user to compare the fingerprint of the telebanking site with the fingerprint on the Financial Certificate to ensure that they match.

There are several offices of accreditation in the Internet sector, but one of the most recognized accreditation offices is the American company, Verisign.[27] Verisign is mostly used by Swiss banks. When a customer connects himself to an Internet Telebanking site, the bank will send the customer a certificate issued by Verisign. The Telebanking site's Internet navigator will then display information related to this certificate, and will ask the customer if he accepts it or not. The customer will be able to make his decision by comparing "the fingerprint" on the certificate sent with the official Financial Certificate, and particularly, the fingerprint on the bank's Internet site.[28] If they are identical, this means that the customer is confident that he will communicate, and send information directly to his bank, and not to the site of a professional hacker. He will be able to accept the certificate as soon as the user "clicks" on the icon labeled "Accept". The communication will then be ciphered and the Internet navigator will code all information sent and will decode all information received. The customer is thereby given assurance that he is

---

26. *See WhyUBS e-banking classic is so secure, supra* note 24.

27. *See* Verisign, *Verisign, at* http://www.verisign.com (2001).

28. *See, e.g.*, UBS, *UBS e-banking classic FAQ Authenticity of the server and the service, at* http://www.ubs.com/e/ebanking/classic/faq/authenticity.html (2001).

communication with his bank and that the information transmitted will remain confidential. However, can the bank trust the user?

2. Verification of User's Identity

For the banks to be sure that the person connected to their protected Internet Telebanking site is the account holder, or an authorized user of the account, the banks must verify his identity. For verification purposes, most banks will request that an individual customer provide three pieces of identifying information, and a corporate customer provide four pieces of identifying information.

a. Contract Number

The contract number is sent to the customer by registered mail after execution of the Telebanking contract. This ensures the bank that the user is a member of the circle of people who know that the contract number will be sent by mail. Obviously, this circle includes the customer of the bank; however, it also includes his spouse, children, the cleaning lady, a workman working in the house, or a robber.

b. Password

The bank also sends a password to it's customer with a request that he modify the password immediately to a word of his choice. This will make it possible to ensure that the bank now communicates only with it's customer or someone who knows him and was able to guess his password. This person could be his wife, one of his children, or a hacker. However, if the customer chooses a random password, memorizes it, and does not write the password anywhere, the risks of "hacking" this password are greatly reduced.

c. List of Numbers or Numbers on Secur ID Card

A number is placed on a list of ninety numbers[29] or on cards called Secur ID cards[30]. Both are sent to the customer through the mail. Using the number list, the customer will be able to validly connect to the Telebanking site. The customer will then cross out the number used for his current connection off the list, and use the next number on the list for the next session. However, because the numbers are contained on a list, it

29. Contrary to UBS that only uses the list of numbers to be crossed out, Crédit Suisse allows its customers to choose between either system.

30. It has the format of a credit card and has a liquid crystal screen, which displays a number.

is easy to photocopy it, enabling several to have the same number at the same time.

If the customer chooses to use the Secur ID cards, he will not be required to do anything once he is connected. The system will only display one number at a time and will change automatically every minute. This allows the bank to be sure that it is communicating with the person who holds that particular number. If the customer chooses a Secur ID card, only the person who is in possession of the card at the time of the connection has access to the number required for connection to the bank. However, if the customer loses his card, he can immediately request that UBS send him a new one. A potential thief would have to also know the customer's personal password, and contract number in order to use the customer's account without his knowledge.

3. Risks of Fraudulent Use of the Telebanking Account

The bank itself can be a fraud as seen in the notorious case of European Bank of Antigua[31]. The European Bank of Antigua enabled two Russians to gain more than ten million dollars in 1997 to the detriment of the unfortunate customers who opened an account at this bank.[32] Thus, before signing a telebanking contract with a bank, and sending funds to a bank, it is wise to investigate the quality of the bank. If this investigation is not carried out, the user connected to the protected Internet telebanking site runs the risk of an unauthorized third party using his account without his knowledge. This situation can occur through the actions of the following three types of individuals: the staff of the bank, a computer hacker (hacker), and the user (if he is negligent by not taking the proper precautions to ensure that each session is confidential).

a. Bank Staff

The people who are at risk on the bank staff are the data-processing specialists who are responsible for the telebanking service because it is possible for them to connect themselves to the account of the customer.

---

31. *See* Savona, *supra* note 1.

32. This massive fraud culminated in August 1997, in the collapse of the European Union Bank (EUB). The police at the time discovered that two mafiosi known to the police services, Alexandre Konanykhine and Mikehail Khodorkoueky were the developers of the world's leading virtual bank as they had declared through aggressive advertising campaigns proposing tax-free interest rates of 9.91%. The target customers were money launderers, as well as, people wishing to evade taxes. The bank of England and the American Bank of Idaho went into action and in August 1997, the Anti-gang authorities opened investigations for fraud. It was however late for the two criminals had already dismissed the banks' five man staff and safely stashed away the ten million dollars which have never been recovered.

Crime statistics indicate that there is a rise in the attacks that are carried out with the help of an internal contact in the company. This is why data processing specialists must be supervised by a sufficiently dissuasive internal police system. While it is relatively easy for the data processing specialists of a bank to enter the account of the customer, and divert funds therefrom; it is also easy for the police to analyze the network and identify any fraudulent conduct on the part of data processing specialists. This is why only an effective monitoring of the data processing specialists makes it possible to prevent internal fraud, and creates a situation of a "cold war" that dissuades any fraud.

There are several ways that a data processing specialist within a bank can assume the customer's identity in order to use his account fraudulently. For example, he could enter the hard drive of the bank's computers which stores the contract numbers, passwords, and the algorithms that are used to generate the numbers "randomly chosen" for the number list or Secur ID cards of customers without the bank's computer being able to identify who hacked into it's hard drives. However, this is almost impossible because the bank's computers would have identified him before he was able to penetrate the hard drives. The machine will keep track of the person's identity by recording his name, the hour and the connection time, as well as the type of action that he takes. If such an action is automatically transmitted to and stored in a safe place, the trail of the fraud will be indelible and usable by the police. The only way to avoid being identified, would require the hard drives to be physically removed, and then analyzed from a computer that is not connected to the bank. However, if the security system that is in place is adequate, the removal of the hard drive will leave traces in the central computer of the bank, or in the designated safe place. The data processing monitoring systems, as well as the internal police devices of the bank, seem to be sufficiently dissuasive for the moment, and make these type of acts very rare. The prospect of the perpetrator being identified in the event of fraud effectively dissuades the data processing specialists who could be tempted to commit such an offense.

Major Swiss banks affirm that they have never been attacked to date.[33] However, other sources have reported contrary information; specifically, that the banks would prefer to bear the burden of any damages,[34] by

33. Based on October 1999 interview with UBS and Crédit Suisse legal departments.

34. There is one central point for carrying out a 'hold-up' the bank's computer server. Before the Internet, gangsters could choose their bank counter. In the event of a hold-up, customers avoided such a bank for a certain time and went to another to carry out their transactions. Today with Internet, in the event of fraud at the 'electronic counter' i.e., the

choosing not to publicly reveal the theft as opposed to tarnishing the image of the bank. Consequently, the banks which have a sufficiently dissuasive internal police mechanism in place, are less likely to be penetrated, and suffer fraud losses by means of an internal contact within the bank.

b. Professional Hackers

i. Decoding of the Transmission and Algorithm Discovery

As for the professional hackers, they work to "break" the encoding keys currently used by the banks in order to decode the SSL coding, and to intercept the data-processing keys authenticating the user.[35] These hackers have the greatest computing power in the world called "CRAY" or "Supercomputer", and recently spent more than one month, working at full capacity, to decode such a key. The user does not usually communicate for more than one hour, and often only for a few minutes with his bank to transmit his orders, and that the keys change each time (numbers on list to cross out or Secur ID cards). Thus, the ability to use the Telebanking account of a customer, without his knowledge, requires the hacker to record the "conversation" between the customer's computer, and that of the bank, and then succeed in decoding it. This will give the hacker the customer's contract number, and password.

Finally, the hacker obtains, through the contact from the bank, the algorithm which "randomly" generates the numbers on the list to cancel or that was displayed every minute on the Secur ID card. This enables the hacker to have all the data-processing keys of the customer. However, under such a theoretically possible option, the hacker would spend so much money to get the hardware necessary for the "hacking" that only the tapping of very significant bank accounts (of at least ten million dollars[36]) would be profitable. Thus, the accounts with lower balances run a substantially lower risk of being the subject of such fraud.

Internet telebanking site, there is no alternative for there is just one choice. The damage to the bank's security through press revelations of such a case of fraud would therefore be greater and would thus provide a strong incentive for the latter to silently pay the victim in order to hush the matter.

35. The film 'Entrapment' released in the spring of 1999 acted out such a scenario: virtual 'hold-up' of a huge sum of money carried out using very expensive computer equipment.

36. Estimated minimum cost of the baseline equipment a hacker should have.

ii. Usurpation of the Identity of the Bank by Creating an Internet Mirror Site with an Official Fingerprint

A simpler means to obtain the data-processing keys of the customer of a bank is to set a data-processing trap to the bank.

a) The Print is Different from that of the Bank

Under this scheme, an Internet site identical to that of the bank would be created but would have a different fingerprint. A customer of the genuine bank would be requested to go to the trap site. While the customer is connected to the trap site, the trap site will communicate the data-processing keys to the hacker.

It is very easy for a hacker to completely recopy the site of a bank. All that the hacker has to do is: go to the bank's site, copy all the, displayed pages and then paste them on his trap site. Moreover, in order to reassure the customer of the security of his information, the trap site of the hacker will have a fingerprint, and certification of server obtained at Verisign. [In order to the simulate Verisign certificate, the hacker is only required to give the impression that his site wants to make an unspecified electronic trade requiring the use of coded transmissions, and to receive the credit card number.] Based on this information, Verisign will grant him the necessary certificate. As soon as the site is installed, the hacker will be able to send an electronic mail to the target customer of the bank informing the customer that the address of the Telebanking site has changed: for example, www.ubs.net instead of www.ubs.ch. If the customer accepts this electronic mail as true, he will then be connected to the trap site of the hacker which appears to be the official site of the bank. The customer will, in all confidence, then transmit his data processing keys through the trap site when he tries to access the Telebanking service. Then, the hacker only has to memorize these data-processing keys as they are being sent. This will give the hacker the ability to immediately use the data processing keys to connect to the genuine Telebanking site of the bank.

If the customer uses the number lists, the hacker will not even need to know the algorithm that generated the information. However, the hacker will only be able to connect to the Internet site of the bank. The next time the following number on the list of numbers will be required, and the hacker will not have access to this information unless he repeats the operation of the trap site, or obtains the algorithm that generated this figure. This would be almost impossible unless the hacker has a contact within the bank. On the other hand, if the customer uses a Secur ID card, the number obtained will be valid for only one minute. After this time

period passes, a new number will be generated. This will force the hacker to get the algorithm of the bank. Yet, in one minute, it is completely possible to memorize the number, and be immediately connected to the legitimate bank site. An easily programmable data processing program can even perform this function automatically. However, this hacking operation is based on one assumption, that the customer will fail to check the fingerprint of his bank, and the fingerprint which is communicated by Verisign during each connection. If the customer regularly verifies this information, he will realize immediately that he is not communicating with his bank. The customer will then refuse to communicate his data-processing keys, because he detects that he is communicating with a trap site.

b) When the Fingerprint on the Trap Site is Identical to that of the Bank

If the fingerprint on the trap site is identical to the fingerprint on the bank's site, the hacker would have a higher success rate in convincing the customer to transmit his data processing keys through the trap site, because the customer would have no means of detecting the data processing trap. This is theoretically possible, but not practical. In order to get a fingerprint identical to that of the bank, there are only few means available to the hacker:

- To "break" into the Internet navigation program of the bank's customer so that the customer will consider the pirate fingerprint as genuine; and the bank's customer will see the same certification of the server when he is connected to the Internet trap site, as that published officially by the bank. Theoretically possible, this seems difficult. One should realize technically, Internet navigators are well designed and not easily modifiable.

- To "break" into the Verisign system itself requires the hacker to obtain from Verisign an authentic certificate that has the same fingerprint as the bank. This process seems technically improbable to the average person because it would require the hacker to have considerable means. Thus, it is very difficult to "break" the Verisign system.

iii. Placing Spy Data Processing Virus in the Customer's Computer

A third means of obtaining the bank's customer's information would be to place a data-processing virus in the customer's computer. This virus would track the "hidden" memory of the Internet navigator, and then back up the data-processing keys of the customer in a non-standard file which is

sent back to the hacker. This is the easiest plan to develop. However, this plan has problems. This plan would only put the hacker in possession of two of the three keys necessary: the contract number, and the password. The numbers intercepted by the data-processing virus would not be useful to the hacker because they could not be used during the next connection to the bank since the number changes each time. Thus, the hacker must get the algorithm generating the number, (a difficult operation, as previously discussed), and photocopy the list of numbers, or steal a Secur ID card. These operations are very risky for the data-processing hacker. Additionally, if the customer erases his "hidden" memory after each session, as recommended by the bank, it largely decreases the risks of infection by such a virus.

c. The Customer is Negligent in Taking the Minimum Necessary Precautions

Lastly, the customer himself represents the largest risk. Indeed, it is much simpler to steal the data-processing keys of the customer than to try to guess them, penetrate the hard drive of the bank, or "break" the encoding system transporting them. Consequently, by choosing an easily imaginable password; by writing it on any medium; by leaving a trail of information (such as his contract number or his list of numbers to cross out, or his Secur ID Card); by not verifying that the official fingerprint of the bank corresponds with that sent by the Internet site certificate during each session; or, lastly, by not erasing his hidden memory after each session, the customer runs a higher risk that his account will be used without his knowledge.

d. The Small[37] *Non-Negligent Customer Runs Almost No Risk of Fraud*

In conclusion, a non-negligent customer of the bank, who takes all the necessary precautions to ensure his data-processing keys are not discovered, and checks the fingerprint of the bank during each session has a very small risk that his account will be subjected to unauthorized use. While the probability that a hacker will penetrate the account of a non-negligent customer or that a bank clerk will use his data-processing keys without his knowledge is very low, the possibility still exists.38

---

37. Meaning having assets in account lower than the cost of the material needed by a hacker to pirate one's account. This amount always change depending on the technological breakthroughs in new increasingly sophisticated hacking gadgets.

38. This is why UBS set up a special security team responsible for constantly analyzing trends in encryption techniques and the means at the disposal of hackers.

However, given the high cost of these "hacking" operations, it is likely that only larger accounts, which contain balances higher than the cost of the hardware that is necessary for the hacking operations, could be affected. On the other hand, if the customer is negligent, he runs a significant risk that his bank account will be used without his knowledge.

4. Tax Risk

A very distinct risk is that tax authorities can discover an undeclared account of one of their taxpayers. The authorities do not have a significant budget to commission good hackers, and to provide the hackers with the necessary hardware to allow them to successfully carry out the hacking operation. Thus, the risk that an administration can intercept a communication between a bank and its customer, and decode if the communication was ciphered with some powerful coding system such as SSL is eliminated. This type of operation is illegal as declared in the Swiss Penal Code in Section 144ss.[39]

However, while the administrations cannot learn the content of the communication, they can determine the identity of those who are making the communication with little effort. [With this information, they can conclude, for example, that Mr. X, living in Zoug, declaring an income, and a fortune of 0. - - SFr., connects everyday between 2:30 p.m. and 10:00 p.m.[40] to the Telebanking site of the UBS.] If phone-tapping is authorized by an examining magistrate due to suspicion that there has been a tax offense,[41] it would be possible, through phone-tapping, to record the IP numbers[42] and then question the Internet access provider as to the identity of its customer. Upon ascertaining the identification of the customer, the tax authorities can order the customer to request from the bank they suspect of having an account, a certificate attesting that he is not the economic beneficiary of any funds. If the customer does not comply with this request, the tax authorities will threaten the customer with

---

39. Code pénal suisse [Swiss Penal Code], Recueil systématique du droit fédéral [Systematic Collection of the Federal Right] [RS] 311.0 art. 144(a), *available at* http://www.admin.ch/ch/f/rs/311_0/a144.html [hereinafter Swiss Penal Code, RS 311.0].

40. Opening hour of the American stock exchange.

41. Without the authorization of such a judge, it would be impossible to obtain these numbers through other means (for example civil procedure) since the federal law on telecommunication forbids the communication of IP numbers in order to protect the private life of individuals connected to the Internet.

42. No attribution for each Internet connection and through which can be determined which customer of the access provider is connected to the Internet, when, where, and for how long?

automatic taxation, or other any other measures needed to compensate for the damage caused by the commission of any tax offense.

Telebanking does not increase this type of a tax risk; on the contrary, it decreases it. A customer who attempts to defraud the tax department through facsimile or telephone orders to his bank, or his account manager, will also be controlled by tax inspectors. These types of transactions make it easier for the tax inspectors to trace the customer's accounts than if the customer conducts his Telebanking through the Internet. These types of transactions will allow tax inspectors to intercept the contents of the transactions that the customer transmits to his bank by facsimile or telephone. Normally, the tax inspectors would only be able to determine the sending, and receiving points of the communication if the customer places his banking orders through the Internet. Consequently, the tax risk remains, but is mitigated with Telebanking because the confidentiality of the information transmitted between the bank, and its customer is almost guaranteed, which makes only the identity of the recipient, and the sender discoverable.[43]

D. Services Offered

Banks currently offer a whole range of services that are accessible via Telebanking. In the future, all the services offered by a normal bank will be available on-line, including the following: loan services, leasing services, financial transactions analysis, Stock Exchange orders, transfers between accounts, blocking of credit card services, the ability to change personal information on the account, and the ability to order banknotes.[44] This evolution is inevitable for banks in order to prevent losing market shares in these fields.

However, to date, banks offer the following services:

- Account information: balance, recent transactions, summaries, evaluation of deposits, etc.;

---

43. This also stands out clearly in Crédit Suisse's general conditions in telebanking. Article. 6.2 states, "although data is transmitted in coded package form, those of the sender and addressee are however not coded...consequently, it is possible for a third party to draw conclusions therefore regarding the existence of a banking relation." Crédit Suisse, *Application for Use of Direct Net from Crédit Suisse*, *available at* http://www.cspb.com/en/onlinebanking/documents/cspb_privat_vertrag_e.pdf (last visited Oct. 19, 2001) (Crédit Suisse form no. 114703, version 1.00) [hereinafter *Crédit Suisse Application*]. The last update of the agreement can be downloaded from Crédit Suisse website, http://www.credit-suisse.com, by clicking on "private clients," then "online services," then "directnet" or "online brokerage" and then by clicking on "download agreement."

44. *See generally* Yellownet, *Yellownet*, *at* http://www.yellownet.ch (last visited Nov. 14, 2001).

- Payments: Transfer of accounts to bank or postal account in Switzerland or abroad;

- Stock Exchange: Immediate transmission of purchase orders, and sales of securities (shares, bonds, and on certain markets, options or warrants). Generally, the covered stock exchanges are the United States, London, Milan, and the Swiss stock exchange. In the long run, all stock exchanges will be covered;

- File transfer: Banks authorize transmission of global orders (transfers, Stock Exchange orders, check orders, etc.) written "off-line" by means of specific financial software, and then transferred to the bank in one block in the form of a coded file;

- Quotes: Raw materials, exchange, and stock exchange price (free). Warning by e-mail or through an SMS message sent on the natel[45] as soon as the price reaches a predefined lower or higher limit;

- News: Financial information published (free) by specialized agencies on the matter: Reuters, Bloomberg; and

- Support (Hotline): In the event of problems that occur in use, breakdown or technical disturbances, the banks usually provide the customer with a special telephone that is permanently accessible. This provides the customer with reassurance, and assists him in solving any possible problems.

E. Advantages/Disadvantages

1. Advantages

a. Cost

The advantageous cost of the operations is incontestably the most solid argument supporting the development of Telebanking. The overhead is low and all the commissions are reduced substantially (50% on the transfers and a percentage of reduction increasing proportionally with the amount of the transaction for the Stock Exchange orders).

b. Speed

Secondly, it is undeniable that a transaction transmitted through Telebanking will be carried out more quickly than a normal transaction because it removes a human being from the intermediary role, and replaces him with a computer that transmits the order directly to the trader's

45 Swiss word for cellular telephone.

assignee. Except in the case of a computer breakdown, the customer will find it beneficial to place his order through a Telebanking service because this will enable him to avoid any delays due to the fault of the intermediary [receipt of several orders at the same time from several different customers by the intermediary, or absence of the intermediary at the time of receipt of the order, or at the time the order is transmitted].

c. Independence

Telebanking allows the customer to place his orders from anywhere. In most countries today, there is a computer within the vicinity that the customer can use to connect to the Internet; and which has the basic configuration necessary to place these orders.

d. Time Flexibility

Lastly, the customer can place orders at his convenience, even outside the normal business hours of the bank. This gives the customer the ability to conduct day trading[46] on markets like the United States (open between 2:30 p.m. and 10:00 p.m., Swiss time) or Japan. Telebanking allows the customers to make stock exchange transactions professionally.[47] Before telebanking, this ability was reserved only to the large account holders of the bank; now, this service is accessible to both large and small account holders.

2. Disadvantages

a. Customers Who Lack Minimum Data-Processing Knowledge

In order to use a Telebanking service, it is necessary for a customer to know how to use a computer, a mouse and to have minimum knowledge about browsing. Sometimes, this can block many potential customers interested in telebanking, because they are afraid of the idea of using a computer. However, most banks try to facilitate access to this service by simplifying, to the extent possible, the operations in order to allow all potential customers to use this service.

---

46. Buying and reselling the same day.

47. Before telebanking, "small customers" of the bank needed to call the bank during business hours to place their orders unless they had a special "phone banking" contract offered recently as an intermediate and supplementary measure to telebanking. The closing hour varied between 4:00 p.m. and 5:00 p.m., so it was virtually impossible for the customer to place an order while studying the market at the time of planning the order given that the American market opened its doors at 3:30 p.m. (Swiss time).

b. Security

It is clear that a risk of unauthorized use of a customer's bank account by an unauthorized third party will exist either, through a Telebanking transaction, or during a transaction carried out by normal means. However, if the customer follows the instructions of the bank by taking the necessary precautions, this risk will be greatly reduced. Additionally, it should not be forgotten that when one communicates with his bank through traditional means, such as the telephone, fax or mail, there is also a risk of interception of the transaction. No transmission system is completely secure. The hold-up of the Post Office of Fraumunster in Zurich, the recent attack of a mail train in French-speaking Switzerland, and the many scandals related to illegal tapping demonstrate that there is always a risk of interception. Lastly, it is obvious that the telephone networks where words are exchanged are more exposed to phone-tapping than those where coded information (with a very high degree of security) is exchanged. Yet, the banks try to limit, or even try to exclude any responsibility in the event of hacking. We will analyze further the validity of the general conditions of the banks used to limit their responsibility in the event of hacking. In my opinion, certain limitations of responsibility are highly subject to criticism, are disproportionate, and thus, make them illegal.

III. FORMATION OF THE CONTRACT

A. In General

Generally, offer and acceptance form a contract. One of the protagonists presents to the other party an offer, i.e. the firm proposal to create a contract. This requires the recipient of the offer to accept the offer, refuse the offer or formulate a counter-offer. The conjunction of the offer, and acceptance creates the assent,[48] which results in the formation of a contract. This practice introduced the system of the "request for offers"[49] or "the invitation to make an offer"[50] into this procedure. The "request for offer" proceeds in the following manner: one of contracting parties sends to the other a pre-formulated contract. If the recipient of this "request of offer" signs it, and returns it to the sender, the party will have tendered an offer for the acceptance of the other contracting party.

---

48. PIERRE ENGEL, TRAITÉ DE DROIT DES OBLIGATIONS [CONTRACTS LAW], p. 192s (1997)

49. DANIEL GUGGENHEIM, 1 LE DROIT SUISSE DES CONTRACTS: PRINCIPES GÉNÉRAUX [GENERAL PRINCIPLES OF SWISS CONTRACT LAW]105 (1991).

50. PIERRE TERCIER, 469 LE DROIT DES OBLIGATIONS [CONTRACTS LAW] 89 (1996).

B. Chronology of the Signature of a Telebanking Contract

Initially, the customer receives a "request of offer" from his bank containing the general conditions which are pre-formulated by the bank. The "request for offer" can be in response to a request from the customer, or the result of a marketing campaign of the bank. At this stage, the parties are not legally bound under the terms of 7 al.II CO[51]. Secondly, the prospective customer signs, and returns to the bank the document, which constitutes an offer, and legally binds him within the meaning of the Article. Thirdly, the bank signs the contract, and returns it to the customer with the data-processing keys that will enable him to start using the telebanking service. This represents the bank's acceptance and forms a legal contract.

C. General Conditions

1. Concept

According to a concept retained by the Swiss legislature of 1881, a contract is negotiated, and discussed point by point. This practice often corresponds to reality. However, this practice has developed a new legal concept known as "contracts of adhesion": one of the parties proposes a pre-formatted contract to which the other can only adhere. These contracts contain general provisions. These provisions are pre-formulated contractual clauses that describe in a general way, all, or part of the provisions contained in possible contracts. These provisions are not, in themselves, a source of the law of the contract; they are autonomous rules that have meaning only if the parties decide to integrate them into their contract. They are written in an abstract way, and have value only if they are accepted.

This hybrid character raises inherent difficulties, particularly in their interpretation. It should be noted that these general provisions can possibly be used to describe usual practices. The judge could be inspired to interpret, or supplement, a contract, provided that the contract is not the expression of a unilateral design.[52] However, the introduction of these general provisions limits contractual freedom, since the customer's

---

51. *See* Loi fédérale complétant le Code civil suisse, Livre cinquième: Droit des obligations [Federal Law Supplementing the Swiss Civil Code, Fifth Book: Code of Obligations], Recueil systématique du droit fédéral [Systematic Collection of the Federal Right] [RS] 220 art. 2, *available at* http://www.admin.ch/ch/f/rs/220/a2.html [hereinafter Code of Obligations].

52. PIERRE TERCIER, 468 LE DROIT DES OBLIGATIONS [CONTRACTS LAW] 116 (1996) [hereinafter 468 LE DROIT DE OBLIGATIONS].

contract contain provisions which were not discussed.[53] For this reason, general provisions will not receive an extensive interpretation; instead, these provisions will be given a rather restrictive interpretation. Because of their function in the economic life of the customer, the general provisions should not be interpreted literally. It is necessary to examine, on a case-by-case basis, the meaning, and goal of the provision in question. If, after such an interpretation, the disputed provision still remains unclear, this lack of clarity will be interpreted to the detriment of the contracting party who wrote the provision.[54]

2. The Inclusion of General Conditions in a Contractual Banking Relationship

To protect the party forced to adhere completely to the general provisions of a telebanking contract, without being able to negotiate them, Swiss Law stated that there is a need for the integration of these general provisions into the contract. Indeed, in order for it to be legally valid, both parties must agree that the general provisions supplement are integrated in the agreement which they made, thereby forming an integral part of the contract. There is total integration when the parties accept the general provisions' conditions without them ("in block"), even if they have taken note of them. This process is, *per se,* illicit: it is not necessary that the parties knew of the contents of the provisions. The only requirement is that the text be available, and accessible to the parties. However, this process involves increased risks.[55]

3. General Conditions within the Framework of the Telebanking Contract

The general provisions of the telebanking contract are completely formulated by the bank, and they will be interpreted against the bank by the judge in the event of a dispute. Moreover, since the customer does not have the possibility of discussing the general provisions with the bank, there is total integration of the provisions. This increases risks for the customer who is forced to accept these provisions, that are sometimes very unfavorable to him, if he wants to carry out his banking operations via telebanking. The validity of the contents of these general provisions will

---

53. DANIEL GUGGENHEIM, LES CONTRACTS DE LA PRATIQUE BANCAIRE SUISSE [SWISS BANKING CONTRACTS LAW] 58 (2d ed. 1993); 468 LE DROIT DE OBLIGATIONS, *supra* note 52, at 59.

54. 468 LE DROIT DE OBLIGATIONS, *supra* note 52, at 61.

55. PIERRE TERCIER, 646 LE DROIT DES OBLIGATIONS [CONTRACTS LAW] 117 (1996).

be addressed during the analysis of the responsibility of the bank contained in chapter VI of this article.

D. Offer

1. Definitions and Concepts

The offer is the first demonstration of will, regardless of the author. It is characterized by the fact that a person, the "pollicitant," proposes to another a contract, making its creation dependent only on the acceptance of the other party.[56] One characteristic of an offer is that it binds its author. The term describing this characteristic is the "obligatory rule of the offer." The offeror puts the recipient in a position to create a contract by acceptance, which is the exercise of a general formative right.[57]

The offer comprises three distinct features:

- It is addressed to the recipient, i.e. to a determined or unspecified person;
- It expresses a legal will to create contract; and
- It should contain all the essential terms of the proposed contract.58

2. Contents

a. Reciprocal and Concordant

The offer and acceptance are governed by Article 3 of the Obligation Code [CO] and must be reciprocal and concordant, which results from Article 1 CO.[59] They are reciprocal when the recipient of both the offer and acceptance is the author of the other. They are concordant when they express the assent of the parties to the same contract terms.[60]

b. Essential Elements of the Contract

For there to be assent, the first necessary element is that the two parties must have agreed on the essential points of the contract. The

---

56. PIERRE TERCIER, 467 LE DROIT DES OBLIGATIONS [CONTRACTS LAW] 89 (1996).

57. PIERRE ENGEL, 42 TRAITÉ DE DROIT DES OBLIGATIONS [CONTRACTS LAW] 194 (1997).

58. *Id.* at 193.

59. *See generally* Code of Obligations, RS 220 art. 1, *available at* http://www.admin.ch/ch/f/rs/220/a1.html. *See also* Code of Obligations, RS 220 art. 3, *available at* http://www.admin.ch/ch/f/rs/220/a3.html.

60. *Id.* at 194.

essential points of the contract are those that must be understood in the "spirit of the parties" so that one is presented with a homogeneous, and autonomous agreement.

There are two kinds of essential elements: Objectively essential elements, and subjectively essential elements.

1) Objectively essential elements:

a) Definition

Objectively essential elements are the elements that should be included to individualize the contract. It is a matter of ascertaining the parties involved in the transaction, and the services that each will promise to perform. If an agreement cannot be reached, there is no contract and the judge cannot find that there is a contract when there clearly is a lack thereof.

b) Telebanking Contract

Whether the telebanking contract contains the essential elements which make the contract sufficient is determined as follows:

(i) Determination of the parties concerned

A link must exist between Mr. X and bank Y. If this link is not established, then the parties are not defined. Consequently, Mr. X must be a customer of bank Y; and to obtain this status, he must have opened an account, and have deposited a minimum amount of funds in that bank.

(ii) The essential obligations of the two parties

The bank:

(1) Has an obligation to communicate and process, within a reasonable time, the orders placed by its customer through the Internet or to a qualified person within the bank.

(2) Has an obligation to take the necessary steps to secure as much of the data-processing network of the bank receiving the orders of the customer.

(3) Has an obligation to use the most advanced techniques of encoding, and to update them regularly in order to communicate with the customer in a private, and confidential way.

The customer:

(1) Has an obligation to agree to be bound by the orders transmitted to his bank through the Internet.

(2) Has an obligation to be quick in transmitting the data-processing keys given to him by the bank in order to prevent their fraudulent use by an unauthorized third party to the detriment of the customer or the bank, which will occur if there is discovery of the coding algorithm.

2) Subjectively essential elements

Subjectively essential elements in a contract are secondary elements, but are elements which the parties have, from the start, considered as a condition of their agreement. Although subjectively essential elements are not a necessary element of the contract, one party, or both, can make them a condition of their contract. If they cannot agree, there is no assent and the judge cannot make a finding that there was assent. In order to be part of the agreement between the parties, the contents of the contract must be sufficiently defined, or at least, sufficiently determinable. The debtor must be able to identify the commitment that he is undertaking. As for determinability, it can rise from objective criteria (e.g. the stock exchange price on a given date) or the choice of a third party, or a party to the contract, insofar as the method does not constitute an excessive restraint on the freedom of the debtor (cf. Article 27 Civil Code [CC])[61]. It goes without saying that the parties can never predict, and regulate, all the elements of their contract. Should a dispute occur, the terms of the contract will be reviewed to attempt to resolve the dispute, and it will be up to the judge whether to supplement the contract. The absence, of subjectively essential provisions in telebanking contracts is explained by the procedure of request for offers, which does not give room for negotiation of any other possible additional provisions desired by one of the parties. However, it is theoretically possible to consider a situation where there is an individualized telebanking contract for each customer allowing the customer to remove or add the clauses. This would make it possible for the contract to have the subjectively essential clauses desired by the bank's customer. However, this possibility is not easy in practice, because it would considerably burden the bank with additional work, and costs in order to offer this option. This conflicts with the prime function of telebanking, which is to reduce the bank's costs and the customer's costs. Moreover, this practice would also make it necessary to create a specialized legal department equipped with many lawyers who are able to analyze, and address the possible disputes that could arise under each contract.

---

61. *Cf.* Code civil suisse [Swiss Civil Code], Recueil systématique du droit fédéral [Systematic Collection of the Federal Right] [RS] 210 art. 27, *available at* http://www.admin.ch/ch/f/rs/210/a27.html [hereinafter Swiss Civil Code].

3. Form

The form of the offer should comply with the format provided for by Swiss Law (Article 11 through 16 of the Obligation Code [CO]).[62] Swiss Law confirms the principle of the freedom of the parties to choose the form of the contract. This means that, except when contrary legal provisions exist, the parties are free to select the form that they wish to give to their contract.

However, Article 16 CO provides that when parties have agreed to use a specific contract form, which is not required by law, the parties will only be bound after the specific contract form is created.63 If a written form is required, without a more precise indication, the parties must observe any provisions relating to written contracts, when the law so requires.

Moreover, according to Article 13 of the CO, the telebanking contract, which is required by law to be in written form, must be signed by all parties upon whom it imposes obligations.64 If the law does not provide otherwise, a letter or a telegram is equivalent to a written contract, provided that the letter or telegram contains the signature of the parties to the contract.

Lastly, according to Article 14 CO, the signature must be handwritten by the parties to the contract.65 A signature that proceeds from some mechanical means will be considered sufficient only in cases where it is allowed by usage, such as when it entails signing written value papers in great numbers. We think for the moment, there is no usage in banking matters obliging to use the written form. However, the procedures required within the framework of the telebanking contract confirm the principle of the requirement that the contract be in the written form. In fact, the bank sends to its customer a pre-formulated contract containing general provisions to be signed and returned to the bank.

It is interesting to note that although a "request for offer" is considered not to have any legal consequences, as long as it is not quoted, it considerably restricts the freedom of the contracting party's choice as to the form of the contract.

---

62. *See generally* Swiss Civil Code, RS 210 arts. 11-16, *available at* http://www.admin.ch/ch/f/rs/210/index.html; *see also* Engel, *supra* note 57, at 196.

63. Code of Obligations, RS 220 art. 16, *available at* http://www.admin.ch/ch/f/rs/220/a16.html.

64. *See* Code of Obligations, RS 220 art. 13, *available at* http://www.admin.ch/ch/f/rs/220/a13.html.

65. *Id.*

E. Acceptance

1. Definitions and Concepts

Acceptance is an affirmative response to an offer or an act by which the recipient of the offer expresses the will to create a contract in accordance with the offer. The acceptor, in our case, the customer of the bank, has the will to declare and sign the contract. In order to be valid, the acceptance must be addressed to the offeror (or to its representative), i.e. at the bank, under the terms, or the requirement, of the reciprocity of the declarations of the will to create a contract. Because the acceptance is an act subject to approval, it is not required to state the essential points of the contract, since it corresponds exactly to the offer that will contain such points.[66]

2. Contents

The acceptance must have the same contents as the offer. If not, the acceptance will not be an acceptance, but a new offer, provided that the acceptance contains the essential elements of a new contract.[67] This situation is, however, not very probable in a telebanking contract. Indeed, it is the bank that wrote the offer, and the customer cannot modify the offer. The customer must agree "in block" to all the terms of the contract and does not have the ability to negotiate them. This means that the customer, through acceptance, is restricted to agreeing to the offer made to him by the bank. Consequently, the telebanking contract is created as soon as the acceptance is forwarded (Article 10 al. I CO).68

In a telebanking contract, the bank sometimes receives an offer from a potential customer. If the bank is interested in contracting with the potential customer, it must return a copy of the contract signed by the authorized individuals, along with the data-processing keys that will make it possible for the customer to use the bank's telebanking services. There can be a time lapse between the mailing of the contract by the offeror, and the reception of the data-processing keys. Crédit Suisse and UBS take between two and three weeks to complete the process.

However, United States banks like E-trade, Schwab, or Datek offer a free service without having accepted the contract, as a whole. For example, at these banks the customer must print the "request for offer"

---

66. PIERRE ENGEL, 43 TRAITÉ DE DROIT DES OBLIGATIONS [CONTRACTS LAW] 200 (1997).

67. GUGGENHEIM, *supra* note 49, at 105.

68. *See* Code of Obligations, RS 220 art. 10, *available at* http://www.admin.ch/ch/f/rs/220/a10.html

and then the bank will instantly give to him the data-processing keys, through the Internet. This will make it possible to access the site immediately, and profit from its free services (stock exchange price on line, information of Reuters, etc.). At this point, the bank has not yet formally accepted the contract, it must still receive the contract, review it and sign it, then return it to the customer. Prior to formal acceptance of the contract, the bank provides free services to the customer.

However, if a Swiss bank, governed by Swiss law, decided to do the same, the fact that the bank offered services without having received the offer of its customer, is not enough to perfect the telebanking contract. At this point, the customer has not yet given any funds to the bank, which is an essential element of the contract. Consequently, the contract would be perfect only when the bank has received funds from the customer, and accepted the customer's offer by sending a signed document to the customer.

This is why, in practice, the banks communicate to the customer their banking coordinates, as well as his new account number, only so the customer can deposit funds only after they have received an offer, and accepted it. From that point, there is only one element lacking to create a valid contract: the surrender of the customer's funds to the bank.

3. Form

We have seen that Swiss Law confirms the principle of freedom to choose the contractual form. Consequently, unless a special form is imposed or reserved, acceptance can be given in any form (see Article 1 II of the CO).69

Since a telebanking contract is a contract of adhesion, which requires it to be in writing, the offer and acceptance must also be made in writing.

IV. QUALIFICATION OF THE CONTRACT

A. Is the Telebanking Contract a Production Contract?

1. Essential Elements of the Production Contract

According to Article 363 CO, a production contract is a contract by which one of the parties (the Contractor) pledges to carry out work, for a price that the other party (the Contracting authority) promises to pay him.[70]

---

69. PIERRE TERCIER, 478 LE DROIT DES OBLIGATIONS [THE LAW OF CONTRACTS] 90 (1996) [hereinafter 478 LE DROIT DES OBLIGATIONS]. *See also* Code of Obligations, RS 220 art. 1, *available at* http://www.admin.ch/ch/f/rs/220/a1.html.

70. Code of Obligations, RS 220 art. 363, *available at* http://www.admin.ch/ch/f/rs/220/a363.html

Thus, the contract necessarily supposes:

- That a party pledges to pay a remuneration; if the contract is made on a purely free basis, we depart from the purview of the production contract; and

- that the other party will pledge to produce and deliver work; this is the characteristic of the service.[71]

Indeed, according to a ruling of the federal Swiss court on February 16, 1938, the contract by which a person hires an architect to work out projects, and plans for remuneration, without entrusting him with another later activity is, in general, a production contract. When work is provided free, it can be a question of a mandate only. The main aspect of a production contract is that the contractor promises work, that is the result of an activity; however, to the characteristics of the mandate, allows the assignee to only commit himself to manage a business, or render services: a result which is not guaranteed. The mandate relates to the contractual relations, presupposing a great reciprocal confidence between parties throughout its duration; so much, that one party cannot impose on the other an undesired continuation of the contract. On the contrary, the production contract, which cannot be canceled at any time by the contractor, though it can be by the Contracting Authority, in general, takes into account the legitimate interest that the contractors have with respect to their commitments for the long term execution of a work.

2. Possible Applications to the Telebanking Contract

One could think that the telebanking contract is a production contract. Indeed, if the transmission of the data is free today, it may perhaps change tomorrow. Moreover, one could expect that the bank guarantees the execution of the orders, which are transmitted to it, and consequently, it pledges a result. Lastly, one could think that another principal function of the bank would be to guarantee security at the time of the communication of information through the Internet. However we will see in the following paragraph why we consider that improbable.

3. Exclusion of the Production contract

a. Absence of the Obligation of Price

The telebanking contract does not meet the first essential condition of the production contract. It is, indeed, not possible to have a production contract which is free. The telebanking contract being per definition free,

---

71. PIERRE TERCIER, 3287 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 406 (1995).

does not meet the requirements for a production contract and, this is not likely to change in the future.

Indeed, the bank encourages it's customers to use telebanking. This service enables it to save money. Especially, because the bank does not need to pay employees to act as an intermediary between the customer and the orderer. However, this service would be less enticing to the customer if the service became a paid service.

Moreover, historically the first experiments of telebanking in Switzerland were a failure because this service, called Videotex, was paid. On the other hand the, Minitel in France which also promotes telebanking, and the Internet today, succeeded in gaining the enthusiasm of the public by the simple fact that the Videotex terminals were given to the public. A marketing strategy, which incorporated free distribution of minitel, led to the success of this type of service in France.

Consequently, this essential condition of a production contract is not met today, and does not appear that it will be in the future. Because this condition is necessary, it is enough to disallow the finding of a production contract. However, in order to buttress the argument for the improbable case where telebanking would become a paid service in the future, we will analyze the second condition, obligation of results.

b. Absence of the Obligation of Results

First, the telebanking contract merely regulates the transmission of the customer's commands to the bank, and fails to regulate the execution of the commands controlled by specific contracts, such as the allocation for credit transfer or the factorage contract on Stock Exchange orders. Moreover since these are mandated contracts, they do not involve the obligation of results.

Secondly, the bank cannot, for technical reasons, guarantee total security at the time of the data-processing communication with it's customer through the Internet. All kinds of problems can, occur, such as: deformation leading to false information on the network; a breakdown linked, for example, to the Year 2000 "bug"; or another type of virus.

This is why banks usually deny any responsibility for the possibility of poor functioning of their data-processing network at the time of execution of the telebanking contract. This article will determine whether this total exemption is contrary to Article 20 CO;[72] and whether too much liability is being shifted to the customer, who is responsible for any

72. Code of Obligations, RS 220 art. 20, *available at* http://www.admin.ch/ch/f/rs/220/a20.html (declaring that a contract or a contract clause, if impossible to perform, is null).

problems that occur, through no fault of the customer. The banks do not want to take the risk of incurring the obligation to make its electronic communications with it's customer safer. As a result, there is no obligation in the telebanking contract. This also disqualifies the contract as a production contract.

B. The Mandate Contract

1. Sources

a. Code of Obligations

The mandate contract is governed by Art. 394-418v CO[73]

b. General Conditions

Moreover, the legal rules applicable to the mandate apply primarily to the enacting of instruments, and the parties may take exception to it. For example, they can do this by adopting general conditions. This is a common practice, especially in the banking sector.[74]

c. Banking Customs

Lastly, insofar as the law refers thereto, the practices and customs are also an indirect source of law. These references are comparatively numerous in mandate law.[75]

Customs are an integral part of the contract because the parties either refer to it expressly or tacitly, or simply by taking part in an activity which is dominated by such customs. Customs make it possible to interpret, and supplement the contract entered into with the bank. In practice, this forms a part of the normal banking operations. Thus, one must admit that there is a procedure for handling the payments of a customer, who opens an account in a bank. Similarly, there also exists a practice that forces the bank, within the framework of a contract of deposit of titles, to undertake routine administrative acts.[76] Thus, by signing a telebanking contract, the bank, and the customer tacitly allow the integration of these customs in the contract.

---

73. *See generally* Code of Obligations, RS 220 art. 394-418, *available at* http://www.admin.ch/ch/f/rs/220/index2.html (discussing definitions, effects of the contract, repudiation, revocation, and other contractual governing principles).

74. PIERRE TERCIER, 3920 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 479 (1995).

75. *Id.* at 480.

76. DANIEL GUGGENHEIM, LES CONTRACTS DE LA PRATIQUE BANCAIRE SUISSE [SWISS BANKING CONTRACTS] (2d ed. 1993).

2. Definition

The mandate is a contract where a person agrees to render services for the interest of another in accordance with their will insofar as the conditions of another contract are not carried out.[77]

According to the Swiss definition, the mandate is an obligations-generating contract that is subject to cases where the mandate refers to only one specified service and is a contract similar to a duration contract. In theory, the mandate contract is formed, subject to payment. Therefore, it becomes a bilateral contract because two services are offered in an exchange-type relationship. Because of the mandate's origin, it is viewed as a "bare contract." Therefore, it is an imperfected bilateral contract, because the assignee alone assumes the principal obligation; and, the employer is bound only to secondary duties.[78]

3. Characteristic Elements

Its definition reveals that, within the framework of the telebanking contract, the mandate contract is comprised of three characteristic elements. The bank has the duty to:

- Take all necessary steps in order to communicate, within a reasonable time, the orders transmitted by its customer, through the Internet, to the computer, or to the person in the bank who is qualified to handle them;
- Take all necessary steps to provide the highest security to the Bank's data-processing network, which receives the customer's commands; and
- Use the most advanced techniques of encoding, and update them frequently in order to communicate with the customer in a private, and confidential manner.

These three elements highlight the obligations of the bank, which is a feature of the mandate contract, and an essential element of the production contract.

a. Transmission of Orders to the Executant within a Reasonable Time

Another essential characteristic of the telebanking contract concerns the orders transmitted to the bank. It is crucial that the operation requested

---

77. PIERRE TERCIER, 3923 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 480 (1995).

78. *See generally* PIERRE TERCIER, 3926-3928 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 480 (1995).

by the customer, whether it be a sale or purchase order for quoted stock or a simple payment, be received correctly, and that it be carried out within an acceptable time frame by either the computer[79], or the person responsible for carrying out.

b. Security of the Bank's Data-Processing Network

The bank must do everything possible to guarantee its customer a maximum-security data-processing network through continuous investment in systems with state-of-the-art technology. However, it would be unrealistic to require a guarantee of absolute security simply because such a degree of security does not exist. Research advances at exponential speeds, making it always possible to open new horizons in "foolproof systems."

c. Security of the Encoded Communication between the Bank and its Customer

The bank must permanently update the encoding technique that is used to communicate with it's customer in order to try to provide the most confidential communication possible. However, total confidentiality is impossible to guarantee. The laws limiting encoding that have been adopted in a growing number of countries, could prevent the bank from following technological developments as closely as may be desired. If a law prohibiting the encoding of data higher than a certain figure were adopted in Switzerland,[80] the banks would be bound by this higher legal standard; and could only adapt their encoding upon the whims of legislative developments, which are lagging in relation to technological developments.

4. Form

There is no special provision regulating the form of the mandate contract. Consequently, the mandate contract is not subject to any special form,[81] even when the mandate requires the completion of a legal document subjected to a particular form. A mandate contract is subjected to the

79. Orders transmitted by the customer linked to NASDAQ, the United States stock market shall be entered into his bank's computer system and then transmitted automatically to the stock exchange computer system via the bank's computer system, thereby eliminating the human execution.

80. This type of law exists in France, New Zealand, Singapore, the United States and other countries.

81. Code of Obligations, RS 220 art. 11, *available at* http://www.admin.ch/ch/f/rs/220/a11.html.

scheme analyzed above relating to freedom of form. The telebanking contract is thus, subjected to the written form.

5. End of the Contract

a. In General

In ordinary cases, the contract ends when the assignee has rendered all the required services. The execution of the contract is, therefore, the extinction of the contract. The parties can provide for separate extinction clauses in their contract; they can subject it to the expiration of a time period, or to a term, or condition. In Articles 404 and 405, the Obligations Code [CO] outlines some extraordinary clauses, the most significant being a termination without reasons.[82]

b. Termination without Reasons

Under the marginal note "Revocation and repudiation," Article 404 al I CO provides that the mandate may be repudiated or revoked at any time.[83] This text remains one of the most discussed in contract law, and recently, a new reading of it was proposed. The original reading was drawn from the origin of the rule, and comparison with foreign law. This unconditional right of cancellation draws its prime significance from the fact that each party has the capacity to terminate the contract. That means that the debtor may not be forced to render the service by resorting to the rules of forcible distraint. This principle is dictated by the nature of the obligation, which implies a personal activity.[84] Consequently, the bank and customer can revoke the mandate at any time.

c. Problem of Compensation

Under the terms of Article 404 al. II CO, "the party which revokes or repudiates the contract at an inappropriate time, must compensate the other for the damage that it causes him."[85] The idea is that, in certain circumstances, the party who terminates the contract should compensate the other party to correct for the termination's effects. This compensation depends on the condition that the cancellation interferes with at an inopportune moment. The formula is too restrictive because it utilizes only

---

82. Code of Obligations, RS 220 art. 405, *available at* http://www.admin.ch/ch/f/rs/220/a405.html.

83. *See* Code of Obligations, RS 220 art. 404, *available at* http://www.admin.ch/ch/f/rs/220/a404.html.

84. *See generally* PIERRE TERCIER, 4132-4137 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACT LAW] 505 (1995).

85. Code of Obligations, RS 220 art. 404(D)(I)(1)(2).

the time factor. The federal Court admits that, in situations where the cancellation causes the other party particular disadvantages, the condition must be carried out as soon as the cancellation without a valid reason is given. Consequently, the following two conditions must be met:

> (1) Termination causes a damage because of the time when it intervenes, and because of the measures taken by the other party. For the assignee, it is a question of measures taken and expenses incurred to execute a given mandate. For the employer, it is a question of new, and unexpected expenditures that he must incur to look for a new assignee.[86]
>
> (2) The party terminating the contract did not give the other any valid reason for doing so. In other words, if there is a just reason for cancellation, repair or compensation is excluded.[87]

When these conditions are met, the party which terminates the contract must repair the damage caused by the inappropriate cancellation, and not by the termination as such. The federal Court concluded that the question must be more broad than one of repairing unnecessarily incurred expenditures and expenses. On the other hand, it is out of the question to claim an allowance for loss of profit. However, in practice, parties frequently decide, contractually and in advance, to fix the amount of the compensation due. This is acceptable, but the amount selected must be commensurate with the damage which can be repaired. Otherwise, the provision places an excessive restriction on the right to terminate.

d. Other Extraordinary Causes

The contract can end for other extraordinary causes. A contract for personal services, for example, may become extinct through one of these events:

- the death of one of the parties, is a situation which should be likened to the dissolution of a legal entity. When the mandate must be executed after the death of the assignee, this poses a particular problem: whether it would be necessary as an extension of Article 245 II of the CO to respect the forms of the provisions on account of death;88

---

86. *See generally* PIERRE TERCIER, 4149-4157 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 507 (1995).

87. *Id.*

88. 478 LE DROIT DES OBLIGATIONS, *supra* note 69, at 90. *See also* Code of Obligations, RS 220 art. 245(D)(1)(2), *available at* http://www.admin.ch/ch/f/rs/220/a245.html.

- incapacity, as of the moment when the party loses the exercise of its civil rights; and
- bankruptcy of a party, even if the procedure is later suspended.

It will be recalled that each party may, in addition, terminate the contract if he has a just reason—in particular, if his partner committed a fault which destroys the relationship of confidence. The precision is hardly worth anything in this field because the right of termination provided for in Article 404 CO applies only to the conditional obligation to compensate the party.[89]

e. Liquidation of the Contract

At the moment when a clause of extinction intervenes, the contractual relationship ends. The parties are released from any obligation and can no longer claim any rights. The law reserves two cases that produce a kind of temporary extension of the contract. First, by virtue of Article 405 al. II CO, "If the extinction of the mandate jeopardizes the interests of the employer, the assignee, his heirs or his representatives are bound to continue management until the employee, his heirs or his representative are able to supply it themselves."[90] When an extraordinary clause of extinction (other than termination) intervenes, the contract ends automatically. Such a situation could be prejudicial to the employer because the rules of good faith obligate the assignee or his rightful claimants to take precautionary measures independent of any contractual relation. This is business management (Article 419 CO) imposed by the law, and entirely subject to the rules of the mandate.[91] Second, under the terms of Article 406 CO, "the employer or his rightful claimant shall be bound as though the mandate still existed, to the operations which the assignee performed before being informed of the extinction of the mandate."[92]

Because termination takes effect in the future, the parties are bound by all the obligations resulting from the contract. The assignee must account for, and restore what he received (Article 400 of the CO).[93] The employer must pay, in accordance with the contract, the fees he owes for

89. *See* Code of Obligations, RS 220 art. 404(D)(I)(1)(2).

90. Code of Obligations, RS 220 art. 405(2)(2).

91. *See* Code of Obligations, RS 220 art. 419, *available at* http://www.admin.ch/ch/f/rs/220/a419.html.

92. Code of Obligations, RS 220 art. 406, *available at* http://www.admin.ch/ch/f/rs/220/a406.html.

93. Code of Obligations, RS 220 art. 400, *available at* http://www.admin.ch/ch/f/rs/220/a400.html.

the operations which were carried out[94] insofar as the mandate is not free. Within the framework of the telebanking contract, the bank could not rightfully liquidate the contract knowing that the contract's extinction would imperil the interests of the customer or his heirs.

For example, take the case of a transfer order transmitted by a customer to his bank via telebanking. The customer dies shortly thereafter. The bank will not be able to refuse to make the transfer to the executant, because the customer is deceased. More importantly, since such a situation has little chance of occurring. The transmission of the orders to the executant, directed by the bank's computer, is generally done very quickly.

V. TELEBANKING-RELATED SERVICES

The telebanking contract deals exclusively with the exchange of instructions between the customer, and his bank. During their implementation, such instructions shall be governed by the usual contracts, such as those in the giro banking and in the commission business. The number of services proposed by the bank should be expected to increase markedly in the future. Indeed, we do not see why the bank would refuse to further profit by eliminating middlemen: for example, in the areas of credit (loan agreement), and consulting (factorage contract). If during the transmission of instructions, the bank or the customer breaches the contract, the provisions of the mandate related to telebanking shall apply. However, if the trader erroneously carries out the order in which he receives the applicable provisions, the special contract rubric applies to any analysis of bank, and customer responsibility. We will, however, briefly analyze the two types of contracts involved, along with the telebanking procedures that are conducted after transactions have been transmitted to the bank.

A. The Giro Banking Contract

1. Definition

When a customer opens an account with a bank, and deposits money on this account, he may wish to make only one deposit. He may also like the bank to service payments. In that case, the customer will open a current account. This establishes a tacit contract in which the bank will handle the customer's payments through commercial documents instead of

94. *See* PIERRE TERCIER, 4159-4167 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 508-509 (1995).

cash. This is the giro-banking contract, to be distinguished from the current account itself.

2. Legal Nature

Thus, the concluded contract thus concluded should be referred to as a long duration general mandate. The bank must accept, and carry out the customer's instructions. The interventions of the customer, called payment order or transfer order allowance in the banking practice, are not a new contract. They are merely instructions the customer gives the bank to carry out a giro banking contract. In other words, the customer's instructions are classified under the giro banking contract framework.

When the customer makes out a payment order, he is asking his bank to pay a certain sum of money to a third party. The third party can be either a customer of this bank, or a customer of another bank. The recipient of the payment order will be able to receive this amount in his own name. The legal situation will be somewhat different depending on whether the recipient is a customer of the same bank, or of another bank.

B. Factorage Contract

1. Definition

When the customer asks his bank to buy or sell stock certificates, the bank deducts a factorage charge. The charge may be fixed,[95] or it may be proportional to the amount of the transaction.[96]

2. Legal Nature

The factorage contract, on the sale side, is the contract where a person undertakes in his name, but on behalf of another, to sell or purchase movable or bills, with entitlement to a fee.[97] This definition reveals that such a contract has the following three characteristics:

> The service promised by the commission assignee shall consist of the sale, purchase, and possibly the exchange of certain goods. The sale shall relate to movable goods or bills. Where other goods are involved, the ordinary rules of the mandate shall be applied. The commission assignee shall make this purchase or this sale in his own name, and

95. Businesses with fixed charges include Youtrade from UBS, e-trade, and Tradepac.

96. UBS charges a fee of 0.6% for transactions less than 250,000 Fr.

97. *See* Code of Obligations, RS 220 art. 425, *available at* http://www.admin.ch/ch/f/rs/220/a425.html.

not in that of the principal. He is thus an indirect representative.[98]

VI. OBLIGATIONS OF THE PARTIES

A. Obligations of the Assignee

The obligations of the assignee (the bank) with respect to the principal (the customer) within the framework of the telebanking contract are of three main types:

(1) To provide the customer the widest possible access to the bank's protected data-processing network by guaranteeing the highest possible confidentiality of communication (thanks to the permanent update of the encoding technique used).

(2) To transmit the customer's orders, within a reasonable time, to the bank staff qualified to carry them out.

(3) To inform the customer as quickly as possible of any disturbance of service: stoppage, slow down in activity, interruption, modification of tariffs, or addition of new services.

To use the general terminology of the mandate contract business, these three principal obligations are distributed as follows:

1. Obligation to Render Service

a. Principles

According to Article 396 I of the CO, the scope of the mandate shall, unless otherwise expressly fixed by the convention, be determined by the nature of the business to which it relates.[99]

b. Obligations arising from a Convention

The scope of the contract is initially determined by the convention, reserved by Article 396 I of the CO. Thus, the substance of the contract is crucial. In this context, the full import of the assignee's obligation to follow his principal's instructions stands out.[100] This is the case with the current telebanking contracts concluded by the intermediary of a convention. The bank is obligated to render the services stipulated in the convention it has concluded with the customer. However, none of the four

---

98. *Id.*

99. Code of Obligations, RS 220 art. 396(C)(I)(1), *available at* http://www.admin.ch/ch/f/rs/220/a396.html.

100. PIERRE TERCIER, 3972 LES CONTRACTS SPÉCIAUX 487 (1995).

documents governing the telebanking contract concluded with UBS makes mention of the bank's obligations. UBS contents itself with stating in the main document, titled *Declaration of Affiliation with UBS 24hr-Banking,* that "the customer thus has access to UBS Phone banking, and telebanking via Videotex or the Internet, depending on the technical device chosen, and the network used."[101] The same applies to the telebanking contract of the Post Office entitled "Yellow Net."

On the other hand, Crédit Suisse "DirectNet" claims that "Anyone who has legitimized himself can access, and use its services" and "whoever has earned legitimacy according to figure 1.1 is considered by the bank authorized to use the Direct Net/Telebanking services. Within the limits of the services, and the mechanism opted for in the user's application, the bank can enable the customer to consult the deposit accounts indicated in the application via Direct Net / or Telebanking. On the other hand, the bank can allow the customer to prepare or accept orders and communications . . . ."[102]

Crédit Suisse undertakes:

- authorization of general access to its telebanking services to whoever has been legitimized;
- allowing consultation of the relevant deposit accounts; and
- accepting the orders and the communications transmitted by its customer.

These are the three services that the bank undertook to render pursuant to the convention signed with its customer. Consequently, if the bank fails to specify all its obligations under the convention, such obligations will be determined by the nature of the business.

c. Obligations Arising from the Nature of the Business

In the absence of a convention, the scope of the mandate shall be fixed, in accordance with Article 396 I of the CO, by the nature of the business.[103] This analysis is governed by the parties' objectives, in particular the result expected by the principal. The question must be examined on a case by case basis. If need be, reference could be made to the practices and Customs of the bank to which the assignee's activity is

---

101. The agreements can be downloaded from the UBS website: http://www.ubs.com.

102. The agreements can be downloaded from Credit-Suisse website: www.cspb.com/en/onlinebanking/documents/noralvertrog_e.pdf.

103. PIERRE TERCIER, 3983 LES CONTRACTS SPECIAUX [SPECIAL CONTRACTS] 487 (1995); *see also* Code of Obligations, RS 220 art. 396(C)(I)(1).

attached. If it goes beyond the contents of the mandate, the assignee shall not be entitled to fees, and unless the business management conditions are met (Article 419ss of the CO); he may even have to repair the resulting damage.[104]

Since the banks crafted none (UBS, Yellow Net) or only some (Crédit Suisse) obligations that fall within the framework of conditions governing the telebanking contract, the nature of the business will determine the contract terms. The bank is obliged to render the following services:

- To give to customer such access to the bank's data-processing network as will allow him to make banking operations. This service will be opened to the customer as soon as he receives the data-processing keys;
- To transmit the customer's orders to the bank staff qualified to treat them; and
- To ensure maximum security in any communication between the bank and the customer.

2. Obligation of Diligence

a. In General

Under the terms of Article 398 al. II CO, the assignee is responsible for proper, and faithful execution of the mandate.[105] This is the general principle which comprises the obligation of diligence. The rule indicates the extent of diligence needed. The mandate shall define the contents of the contract, and set objectives. The obligation of diligence determines how the assignee will carry it out it. The assignee must act as any diligent person would under the same situation, i.e., in an objective manner. This by no means, excludes his adaptation to specific cases. This standard of diligence governs the question of whether the assignee has failed to meet his obligation pursuant to Article 398 I of the CO.[106] This standard is often fixed in a set of ethical or general rules called a code of practice. The rules correspond to the general applied standards in the profession. However, the judge may draw inspiration from them without being limited

---

104. PIERRE TERCIER, 3983 LES CONTRACTS SPECIAUX [SPECIAL CONTRACTS] 487 (1995); *see also* Code of Obligations, RS 220 art. 419 (discussing a manager's rights and obligations).

105. Code of Obligations, RS 220 art. 398(2)(a), *available at* http://www.admin.ch/ch/f/rs/220/a398.html.

106. PIERRE TERCIER, 4013 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 490-491 (1995); PIERRE TERCIER, 4015 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 490-491 (1995).

to them.[107] We did not find guidelines issued by a serious banking association such as the Swiss Association of Bankers. However, banks should examine this matter in the near future, given the growing upsurge in telebanking. Guidelines should judge the level of the requirements, take account of all circumstances (in particular the mandate), reflect adjustments for available time, and reflect the importance of the business, and the qualification of the parties.

A telebanking contract is first a banking mandate, that involves significant, and risky services. The time available for the execution is very short since the bank must promptly transmit the customer's orders for them to be properly carried out. This is particularly true for Stock Exchange orders. Lastly, the assignee (banks) must be particularly qualified to handle the customer's order in an appropriate, and secure manner. We can deduce from this, that the degree of diligence required from the assignee is particularly high.

b. Role of Instructions

The law appears to subject the assignee to the unilateral instructions of the principal. Indeed, according to Article 397 al. I CO, the assignee that received precise instructions cannot, in theory, deviate from them.[108] There are two types of instructions:

(1) Instructions

Instructions are only demonstrations of will, subject to reception. The principal indicates to the assignee, how to perform the services promised in the contract. According to Article 397 al. I CO, the instructions are in theory compelling; thus, the assignee cannot deviate from them except for the following:[109]

(i) Urgent measures

If it is necessary for the assignee to act in order not to jeopardize the interests of the principal, shall he have the right to do so even without instruction? For this, refer to Article 397 al. I CO.[110] The assignee may have the right to do so if the situation was not anticipated by the parties, if circumstances do not allow the assignee to request further instructions from

---

107. PIERRE TERCIER, 4020 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 491 (1995).

108. Code of Obligations, RS 220 art. 397(II)(1)(1), *available at* http://www.admin.ch/ch/f/rs/220/a397.html.

109. *See generally id.*

110. *See generally* Code of Obligations, RS 220 art. 404 (governing termination).

the principal, and if the course of action chosen by the assignee corresponds to the hypothetical will of the principal.

(ii) Unreasonable instructions

If the assignee feels that the instructions given to him are unreasonable, he shall be bound to draw attention thereto. This is part of the duty of diligence, also found in the production contract. If the Master persists, the assignee may divest himself from his responsibility, and even terminate the mandate (see Article 404 of the CO).

(iii) Illicit or socially improper instructions

It goes without saying that the assignee should not follow instructions which would violate the rights of others, or infringe on moralities.[111] His compliance with such instructions is no defense for any civil or criminal liabilities he might incur.

(iv) Instructions contrary to the contract

If the mutual agreement defines the contract framework with precision, the assignee shall have the right not to carry out the different instructions that the principal may subsequently give him. This actually places a restriction on the scope of instructions.

(2) Agreements on the execution

In all the other areas, the "instructions" that the principal may give are only instructions for an offer made to the assignee for the execution of the mandate. The latter shall be bound only if he has accepted these terms. It is sufficient in itself that the parties agree on the general framework of the mandate. It will be incumbent on the assignee to carry it out according to terms, and conditions that he deems appropriate.

3. Obligation of Fidelity

a. In General

By virtue of Article 398 al. II CO, "the assignee shall be answerable to the principal for...the faithful execution of the mandate."[112] This complements the obligation of diligence. It compels the assignee to act in all the circumstances in the supposed interest of the principal. The assignee must do everything that can be reasonably required of him to

---

111. *See* Code of Obligations, RS 220 art. 19, *available at* http://www.admin.ch/ch/f/rs/220/a19.html (freedom to contract within limits of the law); *see also id.* at art. 20, *available at* http://www.admin.ch/ch/f/rs/220/a20.html (illegal contracts are null).

112. Code of Obligations, RS 220 art. 398(2)(a).

uphold the mandate, and abstain from all action that could in some way be detrimental to it.[113]

b. Some Applications

This obligation has many applications, which can also be deduced from the general obligation of diligence. Three of them follow:

(1) Obligation to Inform

The assignee shall regularly inform the employer of the progress of the contract, and notify him of any significant incidents, particularly when those are likely to affect the instructions given. For example, when UBS decides to modify its general conditions, it has the duty to notify its customers of the change (see also Article 17 of the G.C.).[114] When it introduces new credit or other services, it is obliged to give customers this new information.

(2) Obligation to Advise

The assignee shall be bound to regularly advise the principal on the choice of the measures to be taken in the principal's interest. The assignee must dissuade the principal when the principal intends to give or maintain instructions that could be prejudicial to the principal. For example, under the telebanking contract, the bank is bound to advise it's customer to regularly modify his password for security reasons, and not make it accessible to others.

(3) The Settlement of Conflicts

As soon as the assignee indicates that the exercise of his mandate raises a conflict of interests whose outcome could be prejudicial to the mandate, he must refuse the mandate if he has not already accepted it, and later on notify the principal or even terminate the contract.[115] That could be the case if the bank had a deficient software authorizing overdraft, and/or failing to establish a link between the orders made via telebanking, and those via a more traditional means like the telephone or the fax (it is in particular the case of the Crédit Suisse).

---

113. PIERRE TERCIER, 4034 LES CONTRACTS SPÉCIAUX [SPECIAL CONTRACTS] 493 (1995); PIERRE TERCIER, 4037 LES CONTRACTS SPÉCIAUX [SPECIAL CONTRACTS] 493 (1995).

114. UBS, *Basic Conditions for the use of electronic aids*, art. 8, *available at* http://www.ubs.com/e/ebanking/order/conditions.newdialog.0001.Upload1.pdf/conditions.pdf (2001) [hereinafter *UBS Basic Conditions*]. The last update of the agreements can be downloaded from UBS website, http://www.ubs.com, by clicking on "e-banking" and then on "contract documents."

115. PIERRE TERCIER, 4042 LES CONTRACTS SPÉCIAUX 494 (1995).

If the customer makes several orders without having enough money in his account, and the bank's computer system fails to stop them, the bank may believe the customer is misusing the telebanking service. The bank must resolve this conflict of interest by serving a warning or terminating the contract.

4. The Duty of Discretion

Discretion's role varies, depending on the purpose of the contract. In relation to his employer, the assignee has a special duty of discretion which is not expressly stated by the law. It arises instead from the general regime of the contract. This duty is based on the protection of the employer's personality. By discharging his obligation, the assignee may and must have knowledge of intimate or secret facts. On the other hand, the assignee must do everything to avoid disclosure of such facts through him or through third parties. The scope of this duty is very broad (Article 418(d) al. I of the CO). It relates not only to all that the employer entrusts to the assignee, but also to what the assignee learns, stumbles on, or guesses during the exercise of the mandate. It obliges the assignee not only to disclose nothing, but also to guarantee that third parties cannot, without authorization, have knowledge of the information in his keeping. This duty goes beyond the execution of the mandate.[116] During a telebanking operation, the bank and the customer exchange data protected by bank secrecy resulting from Article Forty-Seven of the Federal Law on Banks and Savings Banks (LB): Stock Exchange orders, transfer, consultation of the account, etc. However, this secrecy is not absolutely protected in the case of telebanking, for the following two main reasons:

a. Technical Problems Linked to the Internet in General

For technical reasons related to the Internet in general,[117] the bank cannot guarantee that somebody "is not eavesdropping" on the "computer conversation" which it is carrying on with its customer. However, banks seem nevertheless to guarantee a restriction in this "eavesdropping." They assert that "the spy" may know from where the data is coming from and where it is heading, but that he will not be able to know what is said at the time of the "electronic conversation." even if the customer connects

116. *See generally* PIERRE TERCIER, 4045-4047 CONTRATS SPECIAUX [SPECIFIC CONTRACTS LAW] 494-95 (1995).

117. Historically, the Internet was designed to stand against the destruction of communication in the event of a nuclear war. Consequently, to call from point A (Geneva) to point B (Zurich) one need not necessary remain in Switzerland: all the possible connections between A and B will be used maybe via the United States, Australia, France, or any other country which ensures such a connection.

himself in Switzerland to the computer network of a Swiss bank. The conditions applicable to Crédit Suisse's Direct Net state in particular in their Article 6.2 that:

> [T]he customer also acknowledges that data are transported over an open network (e.g. the Internet) which is accessible to third parties. Data are thus transmitted regularly unchecked across international borders. This also applies to data transfers where both the sender and recipient are located in Switzerland.
>
> Although individual data packages are transmitted in encrypted form, the sender and recipient are not encrypted and thus can be read by third parties. It is therefore possible for a third party to conclude that a banking relationship exists.[118]

The bank can therefore never totally guarantee that nobody will access it's data-processing server, and listen to what is going on. However, the Internet has not changed many things: foreign States, or unauthorized third parties can already listen for a long time (without great difficulty) to the telephone conversations (faxes included) between a bank, and its customer.

b. Encoding

Because encoding techniques are becoming increasingly advanced, States are afraid of not being able to listen to all that goes on, particularly within criminal organizations which can communicate without being susceptible to interception. This is why states tend to restrict the complexity of encoding keys.[119] For example, in 1999, it was considered a crime in the United States and Canada to export a key higher than 128 bits. However, the legislation has been amended since. In France, this limit was fixed at fifty-six bytes.[120] In Switzerland, there is no maximum limit, but given the current trend; it is probable that such a law will be on the

---

118. *Crédit Suisse Application*, *supra* note 43, at art. 62.

119. The higher the capacity of the key, the more the coding process becomes complex and the harder will be to interpret the coded communication.

120. *See* Décret no 99-200 du 17 mars 1999 définissant les catégories de moyens et de prestations de cryptologie dispensées de toute formalité préalable [French executive bill of March 17th, 1999, determining the cryptological means and prestations that do not require any governmental authorization or any filing] *available at* http://www.admi.net/jo/1999/04051.html (JORF/LD page 04051).

agenda.[121] Swiss banks currently use keys of 128 bits, which are considered foolproof.[122] However, should the law suddenly fix the maximum limit, banks will not be able to constantly update their security and will instead always have to conform to the maximum key allowed by the law.

The law on encoding would thus curtail the quality of bank secrecy. Today, a foreigner with a bank account in Switzerland may not necessarily use telebanking from his country if the law of his country forbids him from using the encoding keys of Swiss banks. Consequently, the UBS put the following information on the Internet page, making it possible to download the telebanking contract: "The products and services proposed on this page are not accessible to people residing in the United States, Canada, New Zealand, Australia, Japan and Singapore."

5. Other Obligations

a. The Duty to Submit Reports

Under the terms of Article 400 I of the CO, "the assignee shall, at the request of the employer be bound to submit to him at any time a report of his management." This report is an aspect of the obligation of fidelity. The employer must be able to learn, at any time, how his business is progressing.

b. Obligation to Inform

The assignee must in good time provide any information requested in relation to the mandate; this information must be truthful and complete. The bank fulfills this obligation by informing it's customer, on it's protected server, of the situation and the status of the bank's operations.[123]

c. Obligation to Present Accounts

When the mandate involves the management of financial values, the assignee must at any time be able to give the employer a detailed

---

121. As of August 2001, no such law had been adopted in Switzerland. The reason for that might be that the Swiss banks do no want to be limited in their research for up-to-date and better encryption products.

122. However, they update permanently the level of encryption to maintain it at the "foolproof" level.

123. During stock exchange operations, the bank quickly posts on its server the status of orders transmitted by the customer: seconds after the placing of the order, it is labeled as ' taken care of' meaning the bank has received it and is processing it. Minutes afterwards, it is labeled as 'pending', meaning it is in the financial market system and will be carried out as soon as the period elapses or the market permits. A few hours or at most one day after being executed, it is labeled 'allotted'. Then two days later, the bank labels it as 'billed'.

breakdown of the account with supporting documents. The customer can at any time download a global view of his transactions, the balance of his accounts, and a breakdown of the last operations carried out.

However, that banks do not claim responsibility for the accuracy of information that they transmit to their customers via the Internet network. In our opinion, this exemption is a highly criticizable opinion, and we will dwell on this point in the chapter devoted to responsibility.

d. The Duty to Refund

By virtue of Article 400 al. I CO, the assignee is, at the request of the employer, bound to refund to the employer everything that he received, for the purpose of this management, in whatever capacity required.[124] The obligation, which is imperative, exists throughout the contract; but it takes full significance at the end. The duty to refund is also a consequence of the general obligation of fidelity. To execute the mandate, the assignee must receive a number of documents. Moreover, his role often consists of producing or retrieving documents in order to collect money on behalf of third parties. Consequently, he has the obligation to return the documents. The idea is that he should not enrich himself by executing the mandate, apart from receiving the fees that have been agreed-upon. The obligation targets not only property, but all that assignee may have acquired or received. The only case where the assignee has the right to refuse to satisfy this obligation, is that of the right of lien of 9 DC 895 lien.[125] The assignee may refuse to satisfy this obligation in guarantee of his ordinary fee debts.[126]

(i) Restitution during the mandate

Since the current trend is to personalize the presentation of information on the Internet site for each customer, it will be soon possible for each customer to choose the presentation that he wishes. The customer could send to his bank a diagram on CD-ROM or software via the Internet, explaining how he wishes his various accounts to be presented on the site. He could also ask for the restitution of this CD-ROM.

(ii) Restitution at the end of the mandate

At the end of the mandate, the customer can require the destruction of the bank's data-processing keys. Indeed, if the bank preserves these

124. *See* Code of Obligations, RS 220 art. 400.

125. PIERRE TERCIER, 4045-4058 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 494 (1995).

126. *Id.*

keys, such preservation could be detrimental to the customer in the future; for it represents information sensitive to the customer. Because today the password is increasingly being used to carry out all types of operation,[127] customers will often tend to use the same password or the same type of password (names of flowers, dinosaurs, celebrities, etc.).

The bank's possession of this information can give it the means to enter the private life of the customer, and spy on him without his knowledge. This is particularly prohibited by Swiss Federal data protection law.[128] The bank should give the customer a document attesting the destruction of personal information. This is of special concern because the bank requires the assignee, in the event of termination, to turn in the data-processing keys (Article Nine of the UBS General Conditions). If the Bank demands the return of such information from their customers, the information is important.

B. Obligations of the Employer

1. In General

Within the framework of a mandate contract concluded free of charge, the employer is bound only to the services necessary to keep the assignee from sustaining any loss. This is the subject of Article 402 CO.[129] Because the employer's services do not exist in an exchange relationship with the service rendered, this is a bilateral imperfect contract.[130]

2. The Refunding of the Expenditures

Under the terms of Article 402 al. I CO, "the employer must refund to the assignee, all sums and accrued interests, on advances, and expenses that he incurred for the regular execution of the mandate...."[131] As far as the mandate is concerned, this provision is meant to prevent the assignee from suffering losses through a reduction of his credit. The telebanking

---

127. For example, the personal identification Number (PIN) to withdraw money from the bancomat, used one's VISA card or the alarm or inter-phone codes to enter one's office or house, the password to consult one's e-mail, buy a book on the internet via www.amazon.com or to auction property on www.ebay.com.

128. *See generally* Propriété intellectuelle et protection des données [Swiss Federal Data Protection Law], Recueil systématique du droit fédéral [Systematic Collection of the Federal Right] [RS] 23, *available at* http://www.admin.ch/ch/f/rs/23.html [hereinafter Swiss Federal Data Protection Law].

129. *See generally* Code of Obligations, RS 220 art. 402, *available at* http://www.admin.ch/ch/f/rs/220/a402.html.

130. PIERRE TERCIER, 4095 LES CONTRACTS SPÉCIAUX [SPECIFIC CONTRACTS LAW] 500 (1995).

131. Code of Obligations, RS 220 art. 402(III)(1).

contract leads to a lot of money being saved at the bank. The bank no longer needs to pay managers at exorbitant rates to receive the commands of the customer, and transmit those commands to the qualified people of the bank for processing. In telebanking, the customer indeed transmits his commands to the data-processing server, which automatically transmits the orders. Accepting orders placed via telebanking is a cost-saving operation for the bank. The bank not only receives the orders free of charge, but it deducts less factorage under the telebanking contract. This is why the bank does not ask its customers to refund the expenditures. However, although the bank does not exclude its right to expenditures in its telebanking contract, it can call for their refund if the opportunity arises.

3. Compensation for Damage

Under the terms of Article 402 II CO, the employer "must also compensate the assignee for the damage caused by the execution of the mandate, if he proves that this damage occurred through no fault of his."[132] The provision also tends to guarantee that the assignee does not suffer any loss on account of the execution of the mandate. This rule is applied subject to the following three conditions:

a. Damage

The assignee needs to have suffered damage, an involuntary reduction of his property. The concept is distinguishable from deeds that an assignee must perform in order to discharge his mandate, whatever the origin.

b. In the Execution of the Mandate

This damage must have been suffered not only at the time of the mandate, but in the very execution of the contract. It would, of course, be otherwise if the fault came from the assignee himself.

c. Fault

The employer repairs the damage only if he is liable for a personal fault. This fault may also be presumed. According to case law, a presumed fault analysis would not apply to a free mandate because the employer will have to pay damages even if he committed no fault. In this case, analysis follows the same mode as that of Article 402 II of the CO, relating to the management of businesses.[133] For example, if the

---

132. *Id.* at art. 402(III)(2).

133. PIERRE TERCIER, 4109-4114 LES CONTRACTS SPÉCIAUX [SPECIAL CONTRACTS] 502 (1995).

telebanking software is not powerful, and allows the customer to transmit several orders which seriously overdraw his account, this could create a damage at the bank. The customer will have to repair this damage unless he had good faith during the transmission of his orders, and no time to check the balance in the account.

4. Payment of Fees

By virtue of the law, the mandate is free. Therefore, in principle, the employer is not bound to pay to the assignee the fees corresponding to the services rendered. This was carried over from the time when service was rendered "free of charge," which in itself did not exclude the payment of a bonus on an "honorary" basis. Article 394 al. III CO offers two exceptions to this principle, and the exceptions have become the rule:[134]

a. Under the Terms of a Convention

By virtue of the principle of contractual freedom (Article 19 I of the CO), the parties can agree that the assignee's services will be specially remunerated.[135] This agreement can be express or tacit. It may be contemporaneous with, or after the contract's signing. The assignee must establish the existence of such an agreement. The telebanking contracts analyzed are free, and consequently, their general provisions remain, for the moment, silent on remuneration.

b. By Virtue of Usage

Independent of any special agreement on the matter, the employer shall owe a remuneration when such is the norm. This is admittedly the case, except under particular circumstances, when a person renders service on a purely professional basis: as a lawyer, doctor, chartered accountant, etc. It goes without saying, even in this case, that the parties can also agree that the assignee can agree to render certain services without being paid. However, according to this scheme, the important thing is the extent to which the services rendered by the assignee can objectively be useful to the employer. Actually, the rule can be understood only as an application of the principle outlined in Article 82 CO: the assignee is entitled to remuneration only if, and only insofar as, he carried out the agreed

---

134. *See generally* Code of Obligations, RS 220 art. 394, *available at*http://www.admin.ch/ch/f/rs/220/a394.html.

135. *See generally* Code of Obligations, RS 220 art. 19, *available at* http://www.admin.ch/ch/f/rs/220/a19.html.

services.[136] His remuneration is indeed based on the convention. The convention provides, except where particular rules apply, that it is the services and not their result which pay for the debt. This criterion can nevertheless be taken into account to measure conformity of the services.

The telebanking contract is, for the moment, free. Moreover, lower commissions on the operations carried out via telebanking have provided incentive to customers to use the service. However, when all the customers use this medium of communication, the bank will have the right to require fees of the customer without mentioning those fees under the general contract conditions.

VII. RESPONSIBILITY OF THE BANK ASSIGNEE

A. In General

1. Principles

An assignee's violation of his obligations can lead to civil sanctions. Sanctions vary according to the nature of the duty concerned. First, the employer can refuse to pay all or part of the remuneration. Further, he can demand restitution of the transmitted accounts or goods. He also has the right to require the destruction of information relating to him that is stored in the bank's database (LPD). Lastly, if the contract so provides, the assignee can be held to pay a conventional penalty. Moreover, this is the most typical sanction--the employer can sue for damages. According to Article 398 al.I CO, "the responsibility for the assignee is subject, generally, to the same rules as those of the worker in labor relations."[137] The rule refers to Article 321 E of the CO, which is itself based on the general mode of Articles 97/101 CO.[138]

Consequently, the customer of the telebanking service will be able to do one of the following: 1) Sue the bank for damages; 2) Demand payment in the amount of the conventional penalty, possibly an amount fixed in the contract; 3) Refuse to pay the cost of the services if this falls due one day; 4) Demand restitution of the funds deposited in his account;[139]

---

136. *See* Code of Obligations, RS 220 art. 82, *available at* http://www.admin.ch/ch/f/rs/220/a82.html.

137. Code of Obligations, RS 220 art. 398(2)(a)(1).

138. *See* Code of Obligations, RS 220 art. 321, *available at* http://www.admin.ch/ch/f/rs/220/a321.html (obligation to perform); *see also id* at arts. 97-101, *available at* http://www.admin.ch/ch/f/rs/220/index1.html (effect of non-performance).

139. If the latter are invested for three months by the bank and the customer is forbidden from withdrawing them during this period, since he will be guaranteed higher returns only if he were able to retrieve them at any time, the bank may be forced to hand them back to him before the date.

or 5) Demand restitution of the documents or information related to him as well as the destruction of these in the bank's database. The contracts analyzed, however, mention neither conventional penalty nor service cost.

The bank may also be subjected to other sanctions. The customer may file criminal charges, particularly if there is a breach of trust, a violation of bank secrecy, or a data-processing infringement.[140] A customer may also file an administrative violation charge if the bank violated the legal obligations enabling it to carry on its activity and does not respect the guidelines of the Federal Banks Commission (FCB).[141]

Since this study examines only the legal aspects of the obligations of the telebanking contract, this analysis concentrates on actions for damages. This is the most effective measure taken to repair the damage caused to the employer. One can, however, affirm that in the future, the industry should expect an increase in the other types of sanctions, given the substantial increase noted in data-processing criminality these last years.

2. Individual Liability

Under the terms of Article 321 E I of the CO, "the assignee is liable for the damage that he causes to the employer, either intentionally, or by negligence."142 The provision, in spite of its formulation, is a repeat of the general mode of Article 97 or 41 of the CO.[143] Liability is subject to the following four conditions.

a. Prejudice

The employer must prove that he suffered a damage, for example, an involuntary reduction in his property. Under the terms of Article 99 al. III CO, the law also targets the moral wrong, if the prejudice is sufficiently

---

140. *See* Swiss Penal Code, RS 311.0 art. 318 (breach of trust); *id* at art. 143 (data interception); *id* at art. 143bis (data processing system access); *id* at art. 144bis (data modification or erasure); *id* at art. 147 (fraudulent use of computer); *see also* Loi fédérale sur les banques et les caisses d'épargne [Federal Law on Banks and Savings Banks], Recueil systématique du droit fédéral [Systematic Collection of the Federal Right] [RS] 952.0 art. 47, *available at* http://www.admin.ch/ch/f/rs/952_0/a47 [hereinafter Federal Law on Banks, RS 952].

141. *See* Federal Law on Banks, RS 952.0 art 3, *available at* http://www.admin.ch/ch/f/rs/952_0/a3.html (regulating bank activity).

142. Code of Obligations, RS 220 art. 321(B)(1).

143. *See generally* Code of Obligations, RS 220 art. 97, *available at* http://www.admin.ch/ch/f/rs/220/a97.html (effects of non-performance); *see also* Code of Obligations, RS 220 art. 41, *available at* http://www.admin.ch/ch/f/rs/220/a41.html (general principles of damages).

serious.[144] Such damages may include a reduction of the amount available on the account, if such a reduction is due to improper use or non-increase. This situation may arise from the bank's failure to transmit the customer's orders to the person most qualified to handle them.

b. Violation of the Contract

The employer must establish that the assignee violated one of his obligations. This obligation may be a principal obligation, or an additional obligation. In the case in point, banks are obligated to prevent an abusive use of the customer's account, promptly transmit to the bank's executant all orders transmitted in time by the customer, and guarantee the reliability of this transmission.

c. Causal Relationship

The employer must establish that there is an adequate causal relationship between the violation of the contract, and the prejudice he claims. After ordinary principles are applied, according to the ordinary course of things and the general experiments of life, the violation of the contract must have led to the prejudice. Because the customer uses a data-processing medium, and generally does not need to deal with intermediaries to transmit his orders to the executant of the bank,[145] analysis of the bank's data processing system will be the key to establishing the causal link.

d. Fault

The responsibility to the assignee is breached only if there is negligence or an intentional fault. Thus, it can be a question of any fault, even of a light fault. This fault is presumed under Article 97 of the CO.[146]

When these conditions are met, the assignee must repair the damage in accordance with the general rules governing action for liability (Article 42 CO applicable under the terms of Article 99 al. III CO).[147] This Article

144. *See* Code of Obligations, RS 220 art. 99, *available at* http://www.admin.ch/ch/f/rs/220/a99.html (responsibility for fault).

145. Except where for technical reasons the system is defective and the order is place via the telebanking hotline i.e., by phone and thus to a human being.

146. Pierre Tercier, 4074-4079 LES CONTRACTS SPECIAUX [SPECIAL CONTRACTS] 498 (1995); *see also* Code of Obligations, RS 220 art. 97(A)(I)(1)(1).

147. *See* Code of Obligations, RS 220 art. 42, *available at* http://www.admin.ch/ch/f/rs/220/a42.html (burden of proof for damages); *see also* Code of Obligations, RS 220 art. 99(II)(1)(1) (responsibility for fault).

highlights, in particular, the role which Article 99 II CO can play with regard to free mandates.[148]

3. Third Party Liabilities

The law does not specially treat the assignee's responsibilities towards the third parties he calls upon in the fulfillment of his contract, except from the limited angle of substitution. It is consequently necessary to distinguish between the general principle and the special rule. The substitution rubric is valid only if the assignee has the right to call upon third parties. Otherwise he would be committing a breach involving his personal responsibility. The law expressly provides for the acts of substitutes, for which the assignee is answerable as if they were his, but the rubric is also valid if the third parties are mere auxiliaries. The principle is that the assignee is answerable for the acts of his auxiliaries, in accordance with Article 101 CO, going back to the general rules.149

In the specific case of authorized substitution, the assignee is no longer answerable for the acts of the third parties to whom the execution of the mandate has been entrusted. According to Article 399 II CO, he is answerable only if he personally committed an offense in the choice and instruction of the third party substitute.[150]

Such a situation would be possible if UBS undertook an outsourcing operation (vertical disintegration) with a third party. UBS would delegate the management of its information processing system or the execution of the commands transmitted by its customer. This, however, remains unlikely because of bank secrecy, and the security problems that such a substitution could invite.

a. Regulation

The exercise of action for damages is governed by the usual rules, especially insofar as that action involves regulation. Such an action must be filed within ten years.[151]

---

148. *See generally* Code of Obligations, RS 220 art. 99(II)(1)(1)-(3).

149. *See* Code of Obligations, RS 220 art. 101, *available at* http://www.admin.ch/ch/f/rs/220/a101.html.

150. Code of Obligations, RS 220 art. 399, *available at* http://www.admin.ch/ch/f/rs/220/a399.html.

151. Code of Obligations, RS 220 art. 127, *available at* http://www.admin.ch/ch/f/rs/220/a127.html.

b. Exclusive or Restrictive Liability Conventions

The assignee frequently tries, especially by resorting to the general conditions, to limit or exclude his responsibility. The law does not specifically address this matter in the provisions related to the mandate contract. Thus the general rules apply. Given the peculiarity of the mandate, it is advisable to briefly reiterate them.

1) Unquestionable illegality of the exclusion of responsibility for serious offense

Under the terms of Article 100 al. I CO, the assignee cannot validly exclude his responsibility for serious fault.[152] This rule is not subject to exception, and will be interpreted against the party that drafted the general conditions. Moreover, under the terms of Article 101 III CO, the assignee cannot validly exclude his responsibility for serious fault in relation to the activity of his auxiliaries.[153] Thus, the bank clerks who committed the offense as part of the execution of the telebanking contract, engage the responsibility of the bank.

2) Potential illegality of the exclusion of responsibility for a light offense

Insofar as the exercise of an assignee's activity is governed by a concession granted by the authority, Article 100 al. II CO enables even the judge to consider null the clause which would release the assignee from a light offense.[154] This provision is particularly important for doctors, lawyers and bankers. A judge would be capable of nullifying a clause of the general conditions of a telebanking contract. This would exclude the bank from responsibility in the event of a light offense.

3) Unquestionable illegality of a limitation of responsibility which is contrary to manners or affects the rights of the employer

The validity of these clauses remains subject to the general conditions concerning the purpose of the contract. Since it is contrary to good manners,[155] a limitation of responsibility affecting activities which have a direct relationship with the employer's physical integrity or individual rights would be null.

---

152. *See generally* Code of Obligations, RS 220 art. 100, *available at* http://www.admin.ch/ch/f/rs/220/a100.html.

153. Code of Obligations, RS 220 art. 101(3)(1).

154. Code of Obligations, RS 220 art. 100(2)(2).

155. *See generally* Code of Obligations, RS 220 arts. 19-20.

B. Analysis of Clauses of Exclusion of Responsibility in Swiss Telebanking Contracts Currently in Force

1. Current Supply

The telebanking currently accessible to Swiss consumers can be divided into the following two main types:

a. Traditional Telebanking

Banks offer a range of expanding services via Internet, such as stock exchange transactions, transfers, and consultation of the account. Union des Banques Suisses and Crédit Suisse via its DirectNet service offer this type of telebanking.

b. Specialized Telebanking

At present, only two types of services are offered: Stock Exchange transactions, and bank transfers. Banks or financial institutions offer only stock exchange transactions via Internet. However, the American example, and the current trends spell out a future increase in this figure particularly with the introduction of credit via the Internet.[156]

1) Stock exchange transactions

This mainly involves Tradepac[157] (Union des Banques Suisses), Youtrade[158] (Crédit Suisse) & Swissnetbanking[159] (MFC Merchant Bank LTD.). The customers of these sites can only buy and sell titles. They do not in particular have access to the advice of the bank's financial analysts. This differs from transactions carried out via traditional telebanking.

2) Bank transfers

Only one major institution offers this service: Yellownet[160] (offered by the Swiss Post Office).

2. Comparison of Cases of Exclusion of Responsibility

We decided to compare provisions of telebanking contracts' general conditions of the three leading Swiss companies in order to determine whether the cases of exclusion of responsibility are identical and legal.

---

156. www.loan.com in the United States is particularly experiencing a boom.

157. TradePac is online at http://www.ubs.ch/f/telebanking/trade.html.

158. Youtrade is online at http://www.youtrade.ch.

159. Swissnetbanking is online at http://www.swissnetbanking.com.

160. Postal Suisse's Yellownet is online at http://www.yellownet.ch.

The companies studied are the Union des Banques Suisses,161 Crédit Suisse,162 and the Post Office.

At the Union des Banques Suisses (UBS), three key documents govern the telebanking contract: the general provisions of the bank,[163] the framework conditions related to the use of the data-processing keys,[164] and special conditions related to telebanking.[165] Crédit Suisse (CS) uses two documents to regulate the contract: general conditions,[166] and conditions applicable to DirectNet/Telebanking.[167] Postal Suisse (the Post Office) uses three documents titled respectively: conditions of participation in Yellownet, conditions of participation in the postal account, and Postfinance general conditions.[168]

a. The five cases of exclusion of the responsibility of the bank or the Post Office provided for in the general conditions

The general conditions provide for the exclusion of the responsibility of the bank or the Post Office in the following five principal cases:

1) Damage related to an interruption or a slow-down of the service

a) Cases provided for by the banks and the Post Office

The customer can suffer a loss if he is unable to transmit his order to the bank because its network: is overloaded; has problems; is suspended

---

161. Our analysis is limited to the UBS general conditions of traditional telebanking service, since those of the specialized "tradepac" telebanking services are identical.

162. Our analysis is limited to the Crédit Suisse general conditions of traditional telebanking service, since those of the specialized "Youtrade" telebanking services are identical.

163. *UBS Basic Conditions, supra* note 114.

164. *See generally* UBS, *e-banking*, *at* http://www.ubs.com/e/ebanking.html (last visited November 29, 2001). Data-processing key framework document may be obtained from the author.

165. *See generally* UBS, *Special Provisions for UBS e-banking classic, UBS e-banking smart, UBS e-banking tv and UBS e-banking wap, available at* http://www.ubs.com/e/ebanking/order/conditions.newdialog.0001.Upload1.pdf/conditions.pdf (2001) [hereinafter *UBS Special Provisions*] (contained in same data file as *UBS Basic Conditions, supra* note 114.) The last update of the agreements can be downloaded from UBS website, http://www.ubs.com, by clicking on "e-banking" and then on "contract documents."

166. *See generally* Crédit Suisse, *Welcome to Crédit Suisse Private Banking*, at http://www.cspb.com/ (last visited November 29, 2001). [Parts of this World Wide Web site may be inaccessible from United States Internet connections. General conditions document may be obtained from the author. -Ed.]

167. *Crédit Suisse Application, supra* note 43.

168. *See generally* http://www.yellownet.ch [Parts of this World Wide Web site may be inaccessible due to site security. "Conditions of Participation in YellowNet," "Conditions of Participation in the Postal Account," and "Postfinance General Conditions" may be obtained from the author. -Ed.]

for maintenance; is jammed; has a technical deficiency or transmission errors; is stopped due to disturbance; and has broken down if the customer's telebanking service was interrupted for security reasons, if deficiency comes from the Internet access provider, if the transmitted command was not carried out, or was carried out late, or if the customer lodges a late complaint at his bank. In any of these cases, the banks and the Post Office free themselves from any responsibility. For example, if the customer sends a "market"[169] purchase order via Internet to his bank at 14.00 and the order enters the stock exchange information processing system forty minutes later due to one of the reasons stated above,[170] and in the meantime price increases substantially to 14.40, the customer will buy stock at a higher price than if the order had been registered in time.[171] The bank excludes its responsibility if such a damage occurs.

b) Legality of the exclusion of responsibility in these cases

The damage resulting from an inherent technical problem in any data processing system, from a perfectly justified interruption (security), or from an usual and foreseeable reason (maintenance) must be borne by the customer. The customer accepts the risk that his order may not be carried out on time. However, this exclusion is not admissible when these problems recur very often, when the bank or the post office does not try to solve the problem as quickly as possible, or when the bank or the post office does not try to inform the customer in a reasonable time that his order has not been handled. Even in these cases, the bank excludes responsibility if the customer's Internet service provider fails in its own obligations to his customer. Indeed, in these cases, the bank or the post office would meet their general obligations if they did everything to ensure the prompt transmission of the customer's order to the executant of the bank.

In addition, if the software presenting the data to the customer displays false information, (erroneous balance in hand, distorted confirmation of execution, or assumption of responsibility of command), the customer will suffer a prejudice. For example, the customer could decide to buy shares for $100,000, basing his decision on the balance in

169. Meaning without setting a price limit.

170. Electronic markets like NASDAQ, in the United States, have eliminated human intervention: the customer's order placed via internet is transmitted to the bank's computer system which then transmits it automatically to the stock exchange system, without passing through a person.

171. According to Merrill Lynch (Switzerland) the maximum time allowed to punch the order in the computer system is ten minutes in the case of the American stock exchange and NASDAQ in particular.

his account, when his actual account balance is only $70,000. There will be debit interests to pay, and if the price of the share falls substantially, the bank will require its customer to refund part of the $30,000 that the customer obtained by mistake.

These two damages can be due to a software programming error by the bank. They could also be due to a hacker's modification of the bank's program during the transmission between the bank's Internet site, and the customer's computer.

2) Damage related on the exactitude and entirety of information transmitted by the bank: Cases provided for by the banks and the Post Office

The customer that carries out a banking operation via telebanking, because he bases the transaction on erroneous information provided by his bank or the post office, will suffer significant damage for which the banks, and the post office disclaim any responsibility in advance.[172] Suppose, a person consults his account only sporadically. According to the telebanking site, he has $100,000 in his account. The bank further states on it's site that the current value of the Microsoft share is $100. The customer then places a purchase order limited to $100,000 for 1000 Microsoft shares in order to use all the money of his account. The order is launched and carried out, bringing the customer's account down to $0 and depositing the 1000 Microsoft shares in his name. Now suppose that, because of a deficiency of the bank's data-processing server, the information presented was false. The customer actually had only $80,000. The customer will then, as soon as the problem is solved, have a negative account of balance $20,000, and will consequently have to pay debit interests. Now suppose that the following day, Microsoft is declared a monopoly and the shares fall to $60. The total value of the shares of the customer will go to $60,000, and he will have to refund to the bank the $20,000 lent by the data processing error.

If the erroneous information displayed on the telebanking site is so obvious that it can be spotted by an average person placed in the same circumstances, and that the customer does not notice it, the responsibility for the damage caused could not be placed on the bank. However, if an average user placed in the circumstances would be hard pressed to identify erroneous information, no fault will be ascribed to the customer. Technical risks must be borne by the customer. However, one can hardly compare the delay or the non-fulfillment of an order involving a loss of

172. *See, e.g., UBS Basic Conditions, supra* note 114, at art. 4.; *UBS Special Provisions, supra* note 165, at § I.3.

profit with the display of false personal (balance of the account), and sensitive (price of a share) information on which the customer bases a decision that could involve substantial losses of capital. In such cases, the bank should repurchase its customers' shares and take the damage as it's responsibility in order to guarantee the customer a certain security. How will the customer still dare to carry out transactions via telebanking if he has no guarantees of the minimum reliability of the information he receives from his bank by Internet? We are consequently in agreement with the clause of exclusion of responsibility stipulated by UBS, CS, and the Post Office. We regard the communication of such erroneous information as a light or even serious offense, depending on the cases, and we doubt its legality in the event of litigation.

3) Damage related to the software provided by the bank or the Post Office

a) Cases considered by the banks and the Post Office

The customer can suffer an injury if telebanking software provided by his bank, or the post office does not function. This occurs when the bank encodes the communication between the bank and the customer,[173] when the bank presents to the customer the information transmitted across a faulty network,[174] or when a problem occurs during a data transfer from the Internet site of the bank or the post office to the customer's computer.[175]

Indeed, if the safety of computer communication between the bank's Internet site, and the customer's computer is endangered by defective software, bank secrecy will no longer be guaranteed. A third party could consequently intercept the communication, and note significant information (account number, name and addresses of customer, password, number of contract, balances in account, transmitted banking orders, etc.). The third party could use this information to the customer's detriment.

b) Legality of the exclusion of responsibility in these cases

Before distributing software to their customers, the banks or post office must check the software diligently and do repeated tests. If these tests are rigorous, and are conducted a sufficient number of times, banks cannot be reproached if a problem occurs despite the testing. Some technical risk is indeed inherent in any information processing system, and

---

173. *See, e.g., UBS Special Provisions, supra* note 165, at § I.1.

174. *See, e.g., UBS Basic Conditions, supra* note 114, at art. 4; *Crédit Suisse Application, supra* note 43, at art. 4.5.

175. *See, e.g., UBS Special Provisions, supra* note 165, at § I.3; *Crédit Suisse Application, supra* note 43, at art. 4.5.

the customer must be conscious of it. The customer must accept that risk when he decides to sign a telebanking contract.

However, if the tests are neither strict nor sufficiently numerous, or if the bank or the post office notes the deficiency in the software, but fails to quickly inform the customer of the problem, the bank or Post Office must bear the resulting damage. They have violated their general obligations to give the customer the most powerful computer system and software possible.

Because the risks of data interception, and modification by a computer hacker are for the moment very low, with a likelihood of occurrence similar to that of a *force majeure*, one can accept the exclusion of the responsibility of the bank.

4) Damage related to the non-fulfillment of commitments to third parties

a) Cases considered by banks and the Post Office

Many customers commit to making a payment before a specified date. Institutional customers might commit to buy *n* number of shares within two hours from the time the stock exchange lists a company in which the institution has acquired a large number of shares. If these commitments are not carried out because of an unspecified problem, be it technical or related to data interception, the customer will be subject to sanction for non-fulfillment of his obligation with respect to the third party. This will lead to a loss to the customer, for which the bank excludes any responsibility in advance.[176]

b) Legality of the exclusion of responsibility in these cases

The bank cannot be held responsible for the violation of customers' commitments to third parties, because it is difficult to bring evidence. These transactions often rest on trust and verbal agreements. Indeed, the bank would be taking great risks if it had to pay considerable damages with frequency. Such a scenario could endanger the bank's financial health. The customer must bear these risks related to telebanking. However, in the event of glaring, and excessive error ascribable to the bank or the Post Office, the institution has violated its obligation of diligence. It could then be held to pay all or part of the damage caused to its customer.

5) Damage related to a misuse of the customer's account

a) Cases considered by the banks and the Post Office

176. *See, e.g., Crédit Suisse Application, supra* note 43, at art. 4.9.

Damage can result from an unauthorized third party using the customer's account in an improper way. For this, the banks and the Post Office disclaim any responsibility in advance, particularly if illegal interventions take place in the server of the bank,[177] or of the customer.[178] Further, the banks, and the Post Office disclaim responsibility if the misuse stems from a deficiency of the network operator or of Internet access provider[179] or if a defect of legitimization or an undetected forgery enables a hacker to access the bank's server.[180] The banks, and the Post Office bear no responsibility if the customer or one of his agents has lost the key;[181] if there are unauthorized manipulations of the account,[182] or if the password and/or the list of numbers to be crossed out were wrongly used during the transmission of the data between the bank and it's customer.[183] Finally, the institutions disclaim responsibility if an abuse occurred during the blocking of the account, even if it took place within the usual time frame.[184]

b) Legality of the exclusion of responsibility in these cases

Any person who knows the content of the data-processing keys given by the bank to his customer is capable of misusing the account, and causing significant damage. Moreover, if the customer or one of his agents does not have the mental capacity, he or she is likely to cause damage to the account through inexperience and carelessness.

If the customer made a mistake in writing his password and left his data-processing keys unprotected, no reproach can be made to the bank or the Post Office. Moreover, if a hacker illegally penetrates the bank's Internet telebanking site or that of the Post Office, or if the customer in spite of the best possible computer security arrangement made by the latter, the banks or the Post Office will not assume the risk. If the customer or one of his agents does not have mental capacity, he must inform the bank or the Post Office at the time the contract is signed, or at least make sure their incapacity is mentioned in an Official Journal. The

---

177. *See, e.g., UBS Basic Conditions, supra* note 114, at art. 4; *Crédit Suisse Application, supra* note 43, at art. 4.5.

178. *See, e.g., Crédit Suisse Application, supra* note 43, at art. 4.1.

179. *See, e.g., Crédit Suisse Application, supra* note 43, at art. 4.2.

180. *See, e.g., UBS Special Provisions, supra* note 165, at § I.3; *Crédit Suisse Application, supra* note 43, at art. 4.2.

181. *See, e.g., UBS Basic Conditions, supra* note 114, at art. 2.

182. *See, e.g., UBS Special Provisions, supra* note 165, at § I.3.

183. *Id.*

184. UBS Article 3 D.C.

customer's failure in this duty will rightly clear the bank or the Post Office of any responsibility if the account is misused.

However, if the bank did not take all necessary precautions to upgrade its network with the latest encoding or security, the bank would violate one of its principal obligations. Such a violation would be a serious or light offense, depending on the situation. The gravity of the offense should depend on whether negligence was partial (for example, if the customer left his data-processing keys lying about without taking precautions), or total (not of the fault of the customer).

b. Proportionality and Equity Principles which Water Down the Legality of Exclusions of Responsibility

The principles of proportionality, and equity must control a bank or a Post Office's assertion that it is excluded from responsibility. It is true that technical risks or risks related to hackers cannot be attributed to the bank or the Post Office if the institutions take all possible steps to protect themselves. However, if the damage suffered by the customer is great; if the customer did not commit any offense; and if the bank has sufficient resources to make good the damage without falling into serious financial difficulties, the institution must bear partial damages in all cases. It would indeed be unjust to make a diligent customer sustain huge damages. This is particularly true in the sensitive field of telebanking, where damage could have very serious consequences for the customer (for example, a loss of 85% of a retired employee's fortune - saved all his life - when the retiree has made no error). The bank could, without falling into major financial difficulties, assume this sporadically-occurring damage.

c. Principle of Unfavorable Interpretation against the Party Having Drafted the General Conditions

As we saw above, the general conditions should not be interpreted too literally. It is necessary to examine the sense and the purpose of each provision while basing the analysis on honest use. If, in spite of such an interpretation, the provision in dispute remains ambiguous, this ambiguity will be interpreted to the detriment of the drafting party (namely, the bank).

VIII. CONCLUSION

By following the trends of electronic trade, and the Internet's presence in the world, it is certain that the rapid development of telebanking will continue for years to come. Trends are already appearing. Initially, only major banks or financial companies could afford the luxury

of offering services via Internet. However, small firms are emerging with specialties in only one telebanking service: sales and purchase of stocks. Small firms can now emerge as banks. Barely five years ago, this would have been impossible. Indeed, without a counter, without direct interlocutories to the customers (except in the event of big problem via the Hotline telephone system), and without offering only one type of service, these financial companies could never have been born. Nor could they have survived, from a legal and economic standpoint.

The federal banking commission hardly appreciates the so-called "Swiss banks" whose only links with the country are the name "Swiss bank" spread across the network, and the presence of a mailbox. For example, www.swissnetbanking.com, based at P.O. Box 509 in Geneva, and doing very aggressive advertising in financial newspapers, particularly the Herald Tribune, is especially striking. The existence of this company shows that Internet has made it possible to create virtual Swiss banks based 99% in the United States. One should therefore expect a reaction from Swiss legislators. They will not allow this financial fence to return to countries of origin which, even yesterday, cast a shadow on the money market. Moreover, these upstarts are likely to be removed thanks to the new law on money laundering which came into effect in April, 1998 The law applies to any bank or financial intermediary, including companies offering telebanking services. In addition, the prospects for this new service are frightening *vis-a-vis* employment. If financial intermediaries are no longer necessary for the bank to maximize its profit, what will become of the 120,000 people employed in this vital economic sector of Switzerland? Will computer specialists replace them all? One should expect social reactions to the further development of telebanking.

However, the product seems to be worth the price. The amounts deposited in Swiss banks continue to grow more than 5% annually, and today they total 3 trillion Swiss Francs or 1.8 trillion US$.[185] Telebanking is likely to increase this figure.

In addition, the growing number of telebank users will inevitably increase the potential conflicts between the bank, and its customer, particularly with regard to exclusion of responsibility of the latter. One can thus expect a re-balancing of the forces at play. At present, the general conditions favor the banks, which do not want to guarantee any risks. While hackers doggedly endeavor to pull down bank computer security systems, and foreign financial companies try to take advantage of the Swiss banking usage, by owning a Swiss postal address, Swiss banks,

185. McKinsey & Company, *Banking and Securities—The Swiss Banking Industry*, *at* http://www.mckinsey.ch/aboutus/swisspracticeportfolio/banking.htm (2001).

their customers, and the courts will readily attest that the exclusion of responsibility of banks is abusive and illegal. These will be architects and creators of the first case law on the telebanking contract which, although hardly born, already has a bright future ahead of it.