

# CONSUMER PROTECTION RELATING TO CONTRACTS CONCLUDED ONLINE

# The European Point of View



By Reinhard Steenot\*

## Introduction

The Internet offers consumers the possibility to purchase goods all over the world without having to leave their home. Although buying online creates benefits to suppliers as well as to consumers, it also creates certain risks. Within the European Union consumer protection is realised by obliging the supplier to provide specific information and by allowing the consumer to withdraw from the contract. However such obligations cannot eliminate all risks: for example at this point in time there is no binding European legislation that determines to what extent the consumer can be held liable when his electronic payment instrument is used fraudulently on the Internet, for example, by an unscrupulous vendor.

Although rules aimed at protecting the consumer are incorporated in European Directives, the protection the consumer receives is not always equal in the different Member States. So the question arises which law must be applied when a consumer concludes a contract with a supplier who is established in another Member State. The significance of this question cannot be underestimated. On the one hand it is important for the consumer to know in advance whether he will be able to invoke the protection incorporated in his own legislation, on the other hand it is important for the vendor to know whether it is sufficient to comply with the rules, laid down in the legislation of his own country.

## I. Methodology

This article will give a brief overview of the legislation the European Commission has enacted to protect the consumer concluding a contract online. After discussing the scope of application of these rules, we will examine the information requirements that are imposed on vendors and service providers as well as the consumer's fundamental right to withdraw from

the contract. Further, we will discuss how liability should be divided in case an electronic payment instrument is used fraudulently on the Internet. Finally, we will examine which law applies when the contract is concluded between two parties established in different Member States.

## II. Applicable legislation

In order to determine the protection a European consumer enjoys when he concludes a contract on-line, it is necessary to take into account:

- The European Directive of 20 May 1997 on the protection of consumers in respect of distance contracts;
- The European Directive of 23 September 2002 concerning the distance marketing of consumer financial services;
- The European Directive of 8 June 2000 on Electronic Commerce;
- The European Recommendation of 30 July 1997 concerning transactions carried out by electronic payment instruments.

### A. The Directives concerning distance contracts

The directives concerning distance contracts only apply if a distance contract is concluded with a consumer, i.e. a natural person who is acting for purposes which are outside his trade, business or profession. Whereas the Directive of 20 May 1997 is applicable to most distance contracts relating to the sale of goods and the provision of services,<sup>1</sup> the Directive of 23 September 2002 only applies to distance contracts concerning financial services, such as banking and payment services, credits, insurances and investments.

A distance contract means any contract concluded under an organized distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication (e.g. e-mail, fax, phone, the Internet) up to and including the moment at which the contract is concluded. The definition illustrates that the Directives only apply if the parties do not meet each other before and at the time of conclusion of the contract. Whether the parties meet each other after the conclusion of the contract (e.g. delivery, payment) is irrelevant.

Further, not every contract that is concluded by e-mail falls under the scope of application of the Directives. For example, if a supplier only exceptionally concludes a contract by e-mail with a consumer, at the consumer's request, the contract can not be regarded as a distance contract as it was not concluded under an organized distance sales or service-provision scheme run by the supplier. The consumer therefore will not enjoy the protection incorporated in the Directive.

## B. The Directive on Electronic Commerce

Contrary to the Directives concerning distance contracts, the Directive on Electronic Commerce does not only protect consumers. It protects any natural or legal person who, for professional ends or otherwise, uses an information society service. Further, the Directive is only applicable to information society services, i.e. services (including the on-line sales of goods) that are normally provided for remuneration,<sup>2</sup> at a distance, *by electronic means* (e.g. e-mail, the Internet) and at the individual request of the recipient. Therefore, contracts concluded over the phone or by regular mail do not fall under the scope of application of the Directive.

The Directive applies to service providers established in a member state of the European Union. A service provider is established in the state where he exercises his economic activity, using a fixed establishment for an indefinite period. Therefore, the mere fact that a service provider has a website, hosted in a certain country, does not mean that he is established in that country.

## C. The European Recommendation concerning electronic payment instruments

The Recommendation of 30 July 1997 aims at protecting the holder of an electronic payment instrument, in his relation to the issuer. First of all it is important to emphasize that a Recommendation, contrary to a Directive, is not a binding instrument. Member States are not obliged to incorporate the rules laid down in a Recommendation into their national legislation. Therefore the Recommendation hasn't been a great success in Europe. However in the near future the European Commission will launch a proposal for a directive for a new legal framework for payments in the internal market, which will contain many rules incorporated in the Recommendation and which will be binding upon the Member States.

An electronic payment instrument is described as an instrument enabling its holder to transfer funds, to withdraw cash and to load an electronic money instrument. The term covers both "remote access payment instruments" e.g. payment cards, phone, home and internet banking applications and "electronic money instruments"<sup>3</sup> such as proton (Belgium), Mondex (UK) and the Geldkarte (Germany). The Recommendation does not apply to payments by check nor to credit transfers initiated manually and processed electronically.<sup>4</sup>

The issuer is every person who, in the course of his business, makes available to another person a payment instrument

pursuant to a contract concluded with him. The holder is every person who holds a payment instrument, pursuant to a contract concluded between him and an issuer. As in the Directive on Electronic Commerce every person, even a professional or legal person, enjoys the protection that is incorporated in the Recommendation.

## III. Information requirements

All the above mentioned rules require that certain information is provided. It is important to determine which information must be disclosed, at what point in time, and using which means of distance communication. Further, it is interesting to determine what happens when the supplier does not fulfil its obligation to provide the information required.

### A. The Directives concerning distance contracts

#### 1. *The 1997 Directive*

##### i) *Obligation to provide and confirm information*

According to the Directive of 20 May 1997 on the protection of consumers in respect of distance contracts, it is necessary to make a distinction between the information that has to be provided to the consumer in good time prior to the conclusion of the distance contract and the confirmation of this information, which the consumer must receive after the conclusion of the contract.

Article 4 of the Directive determines which information must be provided in good time prior to the conclusion of the contract. It concerns for example the identity of the supplier, the main characteristics of the goods or services, the price, the arrangements for payment, delivery or performance, and information relating to the existence of a right of withdrawal.<sup>5</sup>

The information must be provided in a clear and comprehensible manner and in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions. More specifically, when the goods are sold over the Internet, the supplier can fulfil its obligation by posting the information on his website in such way that a normal consumer acting with reasonable care can find the information immediately (e.g., using a clear hyperlink that refers to the information).

Article 5 concerns the confirmation of some of the information mentioned in Article 4. Further, the confirmation must contain information on the conditions and procedures for exercising the right of withdrawal, the geographical address of the place of business of the supplier to which the consumer may address any complaints, information on after-sales services and guarantees which exist and the method for cancelling the contract when it is of unspecified duration or a duration exceeding one year. It is important to emphasize that the confirmation must take place in writing or using another durable medium available and accessible to the consumer. Further, the consumer must receive such confirmation, which means that it is not sufficient to make this information available on a website. The information must actually be communicated, for example by sending an e-mail to the consumer containing all relevant information. Further, it must be stressed that the consumer must not receive the confirmation before the conclusion of the contract. It is sufficient that he receives the confirmation in good time during the performance of the contract and at the latest at the time of delivery.

It is clear that the aim of this second obligation to provide information is totally different from the objective of the first. Whereas the obligation to disclose certain information before the conclusion of the contract aims at ensuring that the consumer

can give an informed consent, the second information obligation wants to ensure that the consumer, when he wants to exercise certain rights after the conclusion of the contract, has received sufficient information to do so.

### ii) Sanction

When the consumer doesn't receive the written confirmation of the information, the Directive determines that the consumer must have more time to withdraw from the contract (*infra*). However the Directive does not determine which sanction must be applied in case the information requirements laid down in article 4 are not met. So it is necessary to examine the applicable national acts, transposing the Directive, to find out which sanction applies. For example the Belgian Act transposing the 1997 Directive, does not contain a specific sanction, when the information, provided for in article 4 of the Directive is not made available. Thus, according to common law principles a consumer can only claim compensation when he has suffered damages due to the non-fulfilment of this obligation. It is unlikely that a consumer will claim such compensation.

### iii) Minimum Harmonisation

In this context it is necessary to emphasize that the Directive is based on the principle of minimum harmonisation. This implies that Member States have the possibility to incorporate more stringent rules, i.e. rules offering more protection to consumers, into their national legislation as far as these rules are compatible with the principle of the common market.<sup>6</sup> For example, Belgium has used this opportunity when it determined the sanction in case the supplier does not fulfil its obligation to confirm the required information. More specifically in Belgium one must make a distinction between the situation in which the confirmation does not mention—in bold on the first page and in a frame separated from the text—that the consumer has the right to withdraw from the contract, and the situation in which the other information requirements are not met. In the latter situation, the consumer has, as is the case under the Directive, three months to withdraw from the contract. However, in the first situation the sanction is more severe. The consumer can keep the goods received without having to pay for them! Such sanction does not exist in other Member States.

## 2. The 2002 Directive

The Directive of 23 September 2002 concerning the distance marketing of consumer financial services contains similar obligations for the supplier of financial services. However there are some major differences between the two directives. First, the content of the information that must be supplied is different. The supplier of financial services needs to provide considerable more information. Also he needs to communicate to the consumer the contractual terms and conditions. Further, the confirmation of the information must be communicated in writing or using a durable medium available and accessible to the consumer in good time before the consumer is bound by the conclusion of the contract or any offer. So it is not sufficient that the consumer receives the confirmation in good time *during the performance of the contract*.

Basically the 2002 Directive is based on the principle of maximum harmonisation, meaning that the Member States do not have the possibility to incorporate more stringent rules into their national legislation. However, this does not mean that the national legislation of the different Member States becomes irrelevant. First, it must be emphasized that the Directive itself contains some exceptions to the basic principle of maximum harmonisation, as it enables Member States to maintain or introduce more stringent provisions on prior information

requirements when these provisions are in conformity with Community law. Secondly, the Directive doesn't oblige the Member States to apply a specific sanction in case the supplier doesn't fulfil its obligations. It only determines that Member States *may provide* that the consumer can cancel the contract at any time, free of charge and without penalty when the supplier did not meet its obligations. This means that this sanction will not always apply. For example, according to the Belgian Act transposing the Directive, the consumer only has the right to cancel the contract at any time when the supplier did not communicate the information contained in the Directive *that is considered most essential*.

## B. The Directive on electronic commerce

According to the Directive on Electronic Commerce, one needs to make a distinction between on the one hand the general information that a service provider must render easily, directly and permanently accessible to the recipients of the service and competent authorities (e.g., the name of the service provider, its geographic address, ...) and on the other hand the information that only has to be provided when a contract is concluded online. As for as the latter obligation is concerned, the service provider must clearly, comprehensibly, unambiguously, and prior to the order being placed provide the following information: the different technical steps to follow to conclude the contract, whether the concluded contract will be filed by the service provider and whether it will be accessible, the technical means for identifying and correcting input errors prior to the placing of the order and the languages offered for the conclusion of the contract.<sup>7</sup> Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

The Directive on Electronic Commerce does not determine the sanction in case of non-fulfilment of this obligation. So, common law principles apply, unless national law transposing the Directive contains specific sanctions.

A comparison of these rules to the rules that are incorporated in the Directives concerning distance contracts shows that the Directive on electronic commerce contains some additional information requirements. Therefore, a supplier who sells products over the Internet or provides services over the Internet to consumers must also take into account the Directive on Electronic Commerce. Further, it is important to emphasize that the rules laid down in the Directive on Electronic Commerce also apply when information society services are provided to professionals. However, between professionals, it is possible for the parties involved in the transaction to agree that certain information, which is normally required prior to the placing of the order need not be provided.

## C. The European Recommendation

Article 3 of the 1997 Recommendation determines that the issuer has to communicate to the holder the contractual terms governing the issue and use of the electronic payment instrument. The terms must be set out in writing, or where appropriate in electronic form, in easily understandable words and in a readily comprehensive form. They must be available at least in the official language or languages of the Member State in which the electronic payment instrument is offered. The minimal content of the contractual terms is determined by the Recommendation. The fact that the contractual terms must be communicated means that it is not sufficient to make them available on the internet: the issuer must send them by e-mail.

The contractual terms must be communicated upon the signature of the contract *or in any event in good time prior to delivering the electronic payment instrument*. It is unfortunate that it is possible to consent before receiving the contractual terms. In civil law, it is accepted that a person should be able to take notice of the contractual terms before he concludes the contract.<sup>8</sup> Moreover, the question arises whether this rule is compatible with the European Directive 93/13/EEC that determines in its annex that conditions irrevocably binding the consumer to terms with which he had no real opportunity of becoming acquainted before the conclusion of the contract may be regarded as unfair.<sup>9</sup>

The Belgian Act transposing the Recommendation contains a similar obligation for the issuer, but the contractual terms must be communicated *before the conclusion of the contract*. The Belgian Act is also interesting because it provides for a specific sanction if the contractual terms are not communicated *and* the instrument is later used fraudulently by a third person. In such situation the holder, who did not receive the contractual terms, cannot be held responsible for the consequences of the fraudulent use (Art. 12). However, if the instrument is not used fraudulently there is no specific sanction. Common law principles apply, which means that the contractual terms that were not communicated before the conclusion of the contract are not binding upon the holder.

The proposal for a Directive for a new legal framework for payments in the internal market will determine that the contractual terms must be communicated *before the conclusion of the contract*. In that way it meets the criticism formulated in the past with regard to Article 3 of the Recommendation. However, contrary to the Belgian Act, the proposal will not contain a specific sanction applicable in case of fraudulent use of the instrument.

#### IV. Right of withdrawal

##### A. Basic rule

According to the Directive of 20 May 1997 on the protection of consumers in respect of distance contracts, the consumer has for any distance contract a period of at least seven working days in which to withdraw from the contract without penalty and without giving any reason. The only charge that may be made to the consumer because of the exercise of his right of withdrawal is the direct cost of returning the goods. The period for exercise of this right begins in principle in the case of goods, from the day of receipt by the consumer; in the case of services, the period begins from the day of conclusion of the contract. If the supplier has failed to send the written confirmation, the period is three months and begins in the case of goods, from the day of receipt by the consumer, and in the case of services, from the day of conclusion of the contract. However, if the consumer receives the confirmation within this three-month period, a new seven working day period begins as from that moment.

According to the *Directive of 23 September 2002 concerning the distance marketing of consumer financial services* the consumer has a period of 14 calendar days to withdraw from the



**It is clear that the possibility to impose more stringent rules creates difficult problems for suppliers who want to offer their goods and services all over the European Union.**

contract without penalty and without giving any reason.<sup>10</sup> The period for withdrawal begins either from the day of the conclusion of the distance contract<sup>11</sup> or from the day on which the consumer receives the contractual terms and conditions and the information if that is later than the date of the conclusion of the contract.

##### B. Exemptions

Both directives contain exemptions in which it is not possible for the consumer to withdraw from the contract. For example, the consumer cannot withdraw from a contract relating to financial services whose price depends on fluctuations in the financial market outside the supplier's control, which may occur during the withdrawal period, or from contracts relating to the supply of goods made to the consumer's specifications

or clearly personalized or which, by reason of their nature, cannot be returned or are liable to deteriorate or expire rapidly. Further, the consumer cannot withdraw from the contract for the provision of services if performance *has begun*, with the consumer's agreement, before the end of the seven working day period (1997 Directive) or contracts relating to financial services whose performance has been *fully completed* by both parties at the consumer's express request before the consumer exercises his right of withdrawal (2002 Directive).

##### C. Minimum harmonisation and the prohibition to claim an advance

As already indicated, the 1997 Directive is based on the principle of minimum harmonisation, which means that Member States can incorporate more stringent rules. Once again the Belgian legislator has used this possibility. For example, the Belgian Act states that the consumer has a period of seven working days to withdraw from the contract starting from the day *following* the day on which delivery has taken place or on which the contract relating to services has been concluded (which is one day longer than under the Directive).

Further, the Belgian Act determines that the supplier cannot claim payment or claim an advance as long as the withdrawal period has not expired, which implies that the supplier cannot claim payment before delivery of the goods has taken place.<sup>12</sup> The main advantage of this rule is that consumers, wanting to withdraw from the contract, will not encounter difficulties to get back the amount paid to the supplier. The main disadvantage is that suppliers are often reluctant to deliver goods to consumers as long as they have received payment. A possible solution for this problem, which we find very attractive, consists in blocking the money during the withdrawal period with a trustworthy third party (TTP). This way the consumer, initiating the payment order when purchasing the goods over the Internet, can be absolutely certain that the money will be returned by the TTP when he exercises his right to withdraw from the contract. The supplier is absolutely certain that he will receive payment when the consumer does not exercise his right to withdraw from the contract.



## D. Main disadvantage of minimum harmonisation

It is clear that the possibility to impose more stringent rules creates difficult problems for suppliers who want to offer their goods and services all over the European Union. As discussed in Part VI, the supplier will in many cases have to follow the rules, laid down in the law of the country where the consumer has his habitual residence. More specifically, when a French supplier wants to offer his goods in Belgium, he will have to obey the rules incorporated in the Belgian legislation, which are more severe than those incorporated in the French legislation. As it is practically impossible for small enterprises to understand the rules of all Member States, they will often limit their offer to consumers domiciled in a couple of countries. In this way, one of the main advantages of the Internet disappears.

## V. Fraudulent use of electronic payment instrument on the Internet

When an electronic payment instrument is used fraudulently on the Internet and it is not possible to recover the money from the person acting fraudulently, the question arises who will be liable: the issuer of the instrument or the holder of such instrument? At this point in time the liability is determined by the European Recommendation of 30 July 1997, which is however not a binding instrument. In the future the rules laid down in the proposal for a legal framework for payments in the internal market will apply.

### A. Liability in case of fraudulent use of an electronic payment instrument over the Internet: the Recommendation

#### 1. Transactions taking place without electronic identification of the instrument

In order to determine the liability it is necessary to make a distinction between transactions initiated without the instrument being identified electronically or presented physically and other transactions. As transactions on the Internet always take place at a distance, i.e., without physical presentation, the question arises what constitutes electronic identification. As the Recommendation requires that the instrument itself is identified electronically, identification can only take place by inserting a payment card in an electronic terminal connected to the computer. More specifically, if the holder only communicates the number and the expiry date of his credit card or only keys in a confidential code or similar proof of identity, there is no electronic identification of the instrument.

In the absence of physical presentation and electronic identification of the instrument, the holder cannot be held liable for transactions initiated by a person not authorised to do so. It is the issuer who is liable in its relation to the holder. However, this does not mean that it is always the issuer who bears the financial loss. For example, in practice, the contract concluded between the issuer and the merchant accepting payments by credit card determines that the issuer has the possibility to debit the account of the merchant whenever a consumer disputes a transaction because his instrument that hasn't been identified electronically or presented physically was used fraudulently.

#### 2. Transactions taking place with electronic identification of the instrument

##### i) Notification

In case of electronic identification, it is necessary to make a distinction between transactions carried out before notification of loss or theft and transactions that have taken

place after notification. For the latter, the issuer is responsible, except when the holder acted fraudulently.<sup>13</sup> On the other hand, up to the time of notification, the holder bears the loss up to a maximum of 150 euro, except where the holder acted fraudulently, with extreme negligence, or in contravention of the relevant provisions in the Recommendation.

##### ii) Extreme negligence

The Recommendation does not indicate what should be considered extreme negligence. One could reason that in reality the cases of extreme negligence will mostly be limited to situations in which the holder has acted in contravention of the relevant provisions in the Recommendation. Most important are:

- the obligation to take all reasonable steps to keep safe the electronic payment instrument and the means that enable it to be used (for example if the holder leaves his payment card in his unlocked car, he acts extremely negligent);
- the obligation to notify the issuer without delay after becoming aware of the loss or theft of the instrument; and
- the prohibition to record his personal code in any easily recognizable form, in particular on the electronic payment instrument or on any item which he keeps or carries with the instrument.

In this context the question arises when a personal code is recorded in an easily recognizable form. For example, what to do if a card holder encrypts his personal code in a phone number? In Germany the court of Kassel<sup>14</sup> decided that a card holder that incorporates his PIN in a phone number, written down on a paper in his wallet, acts extremely negligent. In the Netherlands<sup>15</sup> it was decided that a card holder that incorporates his PIN in a phone number, written down in his agenda, containing several phone numbers did not act extremely negligent. It is clear that the circumstances will determine the outcome.

The holder also acts extremely negligent if he doesn't notify the issuer of loss or theft, immediately after becoming aware of loss or theft. So the holder must act promptly as soon as he finds out that his instrument is stolen. As it is impossible to prove the actual knowledge of loss or theft of the instrument, it is sufficient that the holder *should have been* aware of loss or theft. For example, as soon as the holder has received his statements of account, mentioning the fraudulent transactions, he is or at least should have been aware of loss or theft. If several days or even hours pass before notifying the issuer, he will be held liable without upper limit.

It is important to stress that the holder, who notifies the issuer too late, will be held liable for all transactions that have taken place before notification. For example, a card is stolen on February the 1st, the holder becomes aware of the theft on February 10, and notifies the issuer on February 12. He will be held liable without any limitation, not only for the transactions that have taken place between February 10 and 12, but for all transactions initiated before February 12. I find this rule too severe for the holder. First, the question can be raised whether the non-fulfilment of the obligation to notify the issuer immediately after becoming aware of loss or theft must be regarded as an extreme negligence, leading to unlimited liability of the holder. Indeed, such regime is very disadvantageous for the holder as damages can be very high in case of a late notification. Secondly, even if one accepts that late notification constitutes extreme negligence, the holder should only be liable without limitation for the transactions that have taken place after that point in time where he should have notified the issuer,

either because he has become aware of loss or theft, or because he should have become aware of loss or theft of the instrument.

### iii) Burden of proof

Although the question is very important, the Recommendation does not determine who should prove that the holder has acted or did not act in contravention of the provisions of the Recommendation or who should prove the existence or absence of extreme negligence. On the one hand, one could argue that the issuer should prove that the holder was extremely negligent or violated his obligations. But how can the issuer deliver this proof, for example, if the holder denies that he has written his personal code on a paper in his wallet? On the other hand, how can the holder prove that he was not extremely negligent? After all, this supposes the proof of a negative fact.

In several jurisdictions within the European Union,<sup>16</sup> a presumption of extreme negligence is used. The mere fact that a third person has been able to use the instrument protected by a personal identification number lets presume that the holder was extremely negligent. This implies that—once the issuer has been able to prove that the instrument and the personal identification number have been used—the holder must prove the absence of extreme negligence. However, this view is not shared in all countries. In the recent Belgian Act transposing the Recommendation into Belgian law, the legislator explicitly prohibits the use of a presumption of extreme negligence. The mere fact that a third person was able to use the instrument does not prove that the holder was negligent. So it is up to the issuer to provide elements that prove the existence of extreme negligence or fraud of the holder.

## B. Cancellation of payments

The directives concerning distance contracts oblige Member States to ensure that appropriate measures exist allowing a consumer to request cancellation of a payment where fraudulent use has been made of his payment card in connection with distance contracts covered by the Directives. In the event of fraudulent use, the consumer must be recredited with the sums paid or have them returned.

Some authors have argued that this article only concerns payments with cards without a card.<sup>17</sup> More specifically, they reason that this article can only apply when the instrument is used without physical presentation and electronic identification. Personally, I think this interpretation is not compatible with the text of the Directive, which concerns every fraudulent use of a payment card.<sup>18</sup> If one accepts that the Directive applies to every fraudulent use of a payment card, it is clear that the Directive creates a distinction between fraudulent use in the real world (no possibility to cancel payment) and in cyber space (always possibility to cancel payment). However, there is no need for such a distinction, since technological measures allow realizing the same level of security in the real and virtual world, for example when initializing the payment requests a personal code and the identification



**The mere fact that a third person was able to use the instrument does not prove that the holder was negligent.**

of the card through a smart card reader. Therefore, the right to cancel a payment should be limited to situations in which there is no physical presentation and electronic identification of the instrument.

## C. The proposal for a Directive

Contrary to the Recommendation the proposal will not determine explicitly that the holder cannot be held liable in case a transaction takes place without physical presentation and electronic identification of the instrument. Does this mean that the basic liability regime also applies to transactions where the identification of the transaction takes place on the basis of the number and expiry date of the credit card? All depends on the way the definition “payment verification instrument” is interpreted, as the regime allocating liability only applies in case of loss or theft of a *payment verification*

*instrument*. A payment verification instrument is defined as a personalised device or a set of procedures enabling the payment service user (hereafter called holder) to identify him and to authenticate a payment order addressed to his payment service provider (hereafter called issuer) for execution. Isn't it possible to argue that the credit card number and expiry date do not sufficiently identify the card holder and do not sufficiently authenticate the payment order?

In any event, I would find it totally unacceptable that the holder should have to bear the risk for transactions where the instrument is used without physical presentation and electronic identification of the instrument of the holder. In the relation to the holder the issuer must bear the risk. Moreover, I think it is necessary to prohibit the issuer to charge back the amount from the merchant who has accepted payment by transmitting the number and expiry date of the credit card. As has been argued before, such regime will stimulate payment service providers to develop safer payment systems over the Internet.<sup>19</sup>

The basic liability regime incorporated in the proposal resembles the regime laid down in the Recommendation. This implies that one has to make a distinction between transactions taking place before and after notification. After notification it is the issuer who is liable (except when the holder acted fraudulently). The holder is liable for transactions taking place before notification, but his liability will be limited to 150 euro, unless he has acted fraudulently or with extreme negligence, in which situation he will be liable without upper limit.

Contrary to the Recommendation, the proposal contains some rules relating to the burden of proof. When the holder claims that a payment transaction was not authorized, the issuer must at a minimum provide evidence that the payment transaction was authenticated, accurately recorded, entered into accounts, and not affected by technical breakdown or another deficiency. Once this proof is delivered, it is up to the holder to provide factual information or elements which 1) would allow the presumption that he could not have authorized the payment transaction and 2) not have acted with gross negligence or fraudulently. Although it is not necessary to actually prove that one did not authorize the transaction and was not extremely

negligent (it is sufficient to provide facts that allow such presumption) the question arises which information the holder must provide. Is it sufficient to allege that that one was at home when the transaction took place and that someone must have seen the personal identification number when it was keyed in, or is it necessary to give more specific information? In the latter situation it will be very hard to provide elements that allow the presumption that one did not authorize the transaction and was not extremely negligent. The limitation of liability for transactions taking place before notification then becomes purely fictitious.

Anyhow, allocating liability exclusively on the basis of the absence or existence of extreme negligence means that the burden of proof will in reality determine the extent of liability. If one places the burden of proof on the holder, the limitation of liability becomes purely fictitious, especially when specific information is required to allow the presumption that the holder did not authorize the transaction and was not extremely negligent. If one imposes the burden of proof upon the issuer, there will be many cases where the issuer will be liable for all transactions exceeding 150 euro, simply because he hasn't been able to prove the existence of extreme negligence. Therefore, I find it better not to allocate liability exclusively on the basis of the absence or existence of extreme negligence.

In the United States, under the Electronic Funds Transfer Act, the extent of the holder's liability for transactions that have taken place before notification does not depend on whether the holder was extremely negligent. To determine the holder's liability, one has to look at the timeframe within which the holder has notified his institution of the loss or theft of the instrument. More specifically, the consumer is liable for unauthorised transfers only up to a value of 50 USD or the amount of the unauthorised transfer that occurred before notice to the financial institution (whichever is less), if the loss or theft of the access device is reported *within two business days after learning of the loss or theft of the access device*. If a consumer fails to notify the institution within two business days after learning of the loss or theft of the access device, the consumer's liability cannot exceed 500 USD. However, if the consumer fails to report within sixty days of the transmittal of the periodic statement, on which the unauthorised transfers are recorded, he will be responsible for all transactions that have taken place after this period of sixty days and before notification.

Personally, I find the combination of the rules that will be laid down in the European proposal and in the Electronic Funds Transfer Act attractive. More specifically, I think that the liability of the holder of a payment instrument should always be unlimited as soon as the issuer actually can prove that the holder has been extremely negligent.<sup>20</sup> If it is not possible to actually prove the existence of extreme negligence, the liability of the holder should be determined in function of the time frame within which the holder notifies the issuer



***In the United States, under the Electronic Funds Transfer Act, the extent of the holder's liability for transactions that have taken place before notification does not depend on whether the holder was extremely negligent.***

of loss or theft, which implies that a late notification as such cannot constitute extreme negligence.

Such regime has several benefits. First, it becomes impossible that the holder will be held liable for all transactions taking place before notification, simply because he can not provide facts that allow the presumption that he was not extremely negligent. Thus the regime guarantees that the liability of the holder who was not extremely negligent and who notifies the issuer in time is limited. Secondly, the possibility for the issuer to escape liability by proving extreme negligence benefits the system. Holders will know that there is a chance that they will be held liable without limitation when they are extremely negligent. So they will be stimulated to take reasonable steps to keep their instrument safe. Finally, determining the amount of liability in function of the time that goes by after becoming aware of theft or loss ensures on the one hand that the holder always has a good

reason to notify loss or theft (which also benefits the system), on the other hand that the holder will not be held liable for all transactions taking place before notification when he did not notify the payment service provider immediately after becoming aware of loss or theft.

## VI. Private international law

When a consumer concludes a contract on-line with a supplier who is established in another Member State of the European Union, the question arises which law is applicable to the contract. The law applicable to the contract has to be determined according to the Convention of Rome of 19 June 1980 on the law applicable to contractual obligations. Indeed, as for as contractual obligations of consumer contracts are concerned, the country of origin principle,<sup>21</sup> laid down in the European Directive on Electronic Commerce is not applicable.

According to Article 5 of the Convention, a choice of law made by the parties can not deprive the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence. When the contract does not contain a choice of law, the law of the country where the consumer has habitual residence is applicable. However, Article 5 is only applicable if certain conditions are met. More specifically:

- the contract must relate to the supply of goods or services or the provision of credit;
- the contract must be concluded with a consumer; and
- the conclusion of the contract must be preceded in the country where the consumer has habitual residence by a specific invitation addressed to the consumer or by advertising, and the consumer must have taken in his own country all the steps necessary on his part for the conclusion of the contract.<sup>22</sup>

The aim of this rule is to protect the so-called passive consumer, i.e. the consumer who hasn't taken the initiative



to contact a supplier, established in another country. When a contract is concluded over the Internet it is not always easy to determine when the conclusion of the contract was preceded by a specific invitation or advertising in the consumer's country. I believe that this is the case when the consumer received an unsolicited e-mail from the supplier, inviting him to conclude a contract,<sup>23</sup> also when the supplier employed the services of a marketing firm in order to display a banner referring to the supplier's website whenever a certain word is typed in on the website of a search engine.<sup>24</sup> Finally, it is possible to apply article 5 when a hyperlink to the website of the foreign supplier is displayed on the website of another supplier, established in the consumer's country. In all other cases—it concerns more specifically the situation in which the consumer has surfed directly to the website of the foreign supplier or the situation in which the consumer has typed in the name of the foreign supplier on the website of a search engine—it seems not possible to apply the rule, incorporated in Article 5.

Support for this view can be found in a Notice of the European Commission, containing guidelines on vertical restraints,<sup>25</sup> in which the Commission explains under which circumstances a supplier acts actively in the virtual world. Although the difference between active and passive is defined from the supplier's point of view and is explained in the context of a block exemption, it gives a certain insight in the way one must distinguish between active and passive consumers. More specifically, the European Commission states that a supplier acts actively when he sends an unsolicited e-mail to the consumer and when he uses banners or links in pages of providers. On the contrary, the mere possession of an interactive website is not sufficient to define the supplier as an active supplier.

When the rule laid down in article 5 is not applicable, this does not mean that the courts of the country in which the consumer has his habitual residence cannot apply the mandatory rules, laid down in the law of the consumer's country. Indeed, article 7 of the Convention determines that it is always possible to apply the rules of the law of the forum in a situation where they are mandatory.<sup>26</sup> The significance of this rule can not be underestimated as the Regulation concerning the Judicial Competence, the Recognition and the Execution of Decisions in Civil and Commercial Matters determines that the courts of the consumer's country are competent whenever the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State.<sup>27</sup> More specifically, the courts of the consumer's country will be competent as soon as the supplier has a website that makes it possible for foreign consumers to conclude contracts on-line.

Finally, I should mention article 12 of the Directive on the protection of consumers in the respect of distance contracts, according to which the consumer can not lose the protection granted by the Directive by virtue of the choice of the law of a non-member country as the law applicable to the contract as far as the contract has close connection with the territory of one or more Member States. This rule is particularly important when the contract was concluded with an active consumer and the courts of the country where the consumer is domiciled are not competent.

## Conclusion

European law contains many rules aimed at protecting consumers who conclude contracts on-line. Not only must consumers be informed, they also must have the possibility to

withdraw from the contract without penalty and without giving any reason. In the future European law will also contain binding rules protecting holders whose electronic payment instrument is used fraudulently on the Internet. However, the protection of the holder of an electronic payment instrument is not guaranteed. Will the holder be able to provide facts that allow the presumption that he did not authorize the transaction and that he did not act extremely negligent? Further, will one accept that a credit card number and an expiry date do not sufficiently identify the holder and authenticate the transaction and therefore transactions taking place without physical presentation and electronic identification of the instrument cannot lead to the liability of the holder?

Finally, it is necessary to realize that—as some Directives are based on the principle of minimum harmonisation—the rules laid down in the national acts transposing the Directives may differ from country to country. Further, the sanctions to be applied will often be different. This makes it difficult for suppliers to offer their goods and services to consumers in different Member States, as they have in many cases, taken into account the rules of private international law, to obey the rules laid down in the law of the consumer's country. Therefore, it is best to harmonize consumer law completely (maximum harmonisation). Another option could be to apply the country of origin principle, incorporated in the European Directive on Electronic Commerce, to contractual obligations of consumer contracts. However, this solution is not attractive as it can deprive the consumer from the protection he enjoys in his own country.

\* Professor of Consumer Law, Ghent University, Belgium, Reinhard.Steennot@ugent.be.

1. The exemptions are enumerated in article 3 of the Directive.
2. The mere fact that a service is delivered for free does not imply that it cannot be regarded as information society service. It is sufficient if it is normally provided for remuneration.
3. Some of the provisions incorporated in the Recommendation do not apply to payments effected by means of an electronic money instrument. However, where the electronic money instrument is used to load (and unload) value through remote access to the holder's account, the Recommendation is applicable in its entirety.
4. The proposal will also apply to credit transfers that are initiated in writing.
5. Unless of course such right does not exist (infra).
6. Meaning that the restriction of free trade resulting from these more stringent rules must be justified by reasons of general good.
7. These rules do not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communications.
8. X. FAVRE-BULLE, *Les Paiements transfrontières dans un espace financier européen*, Basel, Helbing & Lichtenhahn, 1998, 167.
9. M. VAN HUFFEL, "Moyens de paiement et protection du consommateur en droit communautaire et en droit belge", *D.C.C.R.* 2000, 27.
10. However, this period shall be extended to 30 calendar days in distance contracts relating to life insurance covered by Directive 90/619/EEC and personal pension operations.
11. Except in respect of said life insurance, where the time limit will begin from the time when the consumer is informed that the distance contract has been concluded.
12. However it is accepted that a supplier can suggest and therefore accept payment within this period, for example by giving the consumer several possibilities to pay within the



withdrawal period and only one possibility to pay afterwards.

13. The issuer must prove that the holder has acted fraudulently.

14. AG Kassel 16 November 1993, *W.M.* 1994, 2110.

15. GCB 24 September 1994, *T.V.C.* 1995, 183.

16. For example in Germany where one applies the theory of the *Anscheinsbeweis*: OLG Celle 27 februari 1985, *W.U.B.* 1985, 95; C.P. SCHNEIDER, *Point of Sale-Zahlungen mit der ec-Karte*, Konstanz, Hartung-Gorre Verlag, 1990, 156-159; D. SPALLINO, "Rechtsfragen des Netzgeldes", *W.M.* 2001, 238.

17. M. VAN HUFFEL, *o.c.*, 107.

18. See also : B. DE NAYER, "La loi du 25 mai 1999 modifiant la loi du 14 juillet sur les pratiques du commerce et sur l'information et la protection du consommateur: un cadre cohérent pour le commerce électronique en Belgique?", *D.C.C.R.* 1999, 342.

19. A. SALAÜN, "Transposition de la directive contrats à distance en droit belge: commentaire de l'article 20 de la loi du 25 mai 1999", *J.T.* 2000, 44.

20. The issuer can not prove the extreme negligence by invoking a presumption of extreme negligence.

21. The country of origin principle means that a supplier established in a Member State must in principle only obey the rules laid down in his own Member State, even if he offers his services through the Internet in other Member States.

22. The specific rule also applies in some other situations. However, these are not relevant for contracts concluded on-line.

23. R. SHU, "The applicable law to consumer contracts made over the internet: Consumer protection through private international law", *Int. Journ. Law Inf. Tech.*, Vol. 5, 210-211.

24. See also L. ROLIN JACQUEMINS en T. VERBIEST, "L'offre de services et produits financiers sur internet", *R.D.A.I.* 2000, 5; F. SWEERTS, "Internet - Les sites bancaires veulent s'ouvrir au consommateur européen", *Bank Fin.* 2000, 262.

25. Commission Notice, *Guidelines on Vertical Restraints*, 11-12.

26. Y. BRULARD en P. DEMOLIN, "Les transactions commerciales avec les consommateurs sur internet", in *Internet face au droit*, Namen, Story-Scientia, 1997, 48; F. RIGAUX en M. FALLON, *Droit international privé*, T. II, Brussel, Larcier, 1993, 574; W. KOHTE, "Verbraucherschutz im Licht des europäischen Wirtschaftsrecht", *EuZW* 1990, 153; B. KLINGSPORN, "Der Schutz des Verbrauchers im internationalen Privatrecht", *W.M.* 1994, 1098. Contra: BGH 19 maart 1997, *EuZW* 1997, 412; W.F. EBKE, "Erste Erfahrungen mit dem EG-Schuldvertragsübereinkommen", in *Europäisches Gemeinschaftsrecht und Internationales Privatrecht*, Köln, Carl Heymann, 1997, 100-102; P. LAGARDE, "Le nouveau droit international privé des contrats après l'entrée en vigueur de la Convention de Rome du 19 juin 1980", *R.C.D.I.P.* 1991, 316.

27. As far as the contract falls within the scope of such activities.