Financial Law Institute

Working Paper Series

WP 2010-12

Reinhard STEENNOT

Allocating liability in case of fraudulent use of electronic payment instruments and the Belgian mobile payment instrument pingping

July 2010

WP 2010-12

Reinhard STEENNOT

Allocating liability in case of fraudulent use of electronic payment instruments and the Belgian mobile payment instrument pingping

Abstract

In case of fraudulent use of an electronic payment instrument the question arises who bears the financial consequences of such losses. Since in most cases it is impossible to determine who committed fraud, the loss will have to be allocated between the payment service user and the payment service provider. The first part of this article will focus on the rules (incorporated in the new Payment Services Directive) (Kierkegaard, 2007; Vanden Bosch and Mathey, 2007) determining who is liable in case of fraudulent use of a traditional electronic payment instrument, such as a debit card, a credit card or an e-banking system. In doing so, we will especially focus on the concept of extreme negligence and the problems concerning the burden of proof. In the second part of this article we will discuss the applicability of these rules allocating liability to mobile payment instruments, using the new Belgian payment system "pingping" as an example.

Allocating liability in case of fraudulent use of electronic payment instruments and the Belgian mobile payment instrument pingping

Reinhard Steennot

Financial Law Institute, Ghent University

Introduction

1. In case of fraudulent use of an electronic payment instrument the question arises who bears the financial consequences of such losses. Since in most cases it is impossible to determine who committed fraud, the loss will have to be allocated between the payment service user and the payment service provider. The first part of this article will focus on the rules (incorporated in the new Payment Services Directive[1]) (Kierkegaard, 2007; Vanden Bosch and Mathey, 2007) determining who is liable in case of fraudulent use of a traditional electronic payment instrument, such as a debit card, a credit card or an e-banking system. In doing so, we will especially focus on the concept of extreme negligence and the problems concerning the burden of proof. In the second part of this article we will discuss the applicability of these rules allocating liability to mobile payment instruments, using the new Belgian payment system "pingping" as an example[2].

The importance of the rules allocating liability, incorporated in the Directive, must not be underestimated. First, it must be stressed that fraudulent transactions occur quite often. A recent study of the European Commission has shown there are 10 million fraudulent transactions with payment cards in the SEPA area per year, representing roughly €1 billion losses[3]. Secondly, it is important to understand that it is the first time that the European legislator has enacted binding rules concerning the allocation of liability in case of fraudulent use of an electronic payment instrument. Before the Directive, there was only a non-binding Recommendation[4], which has not been very successful in Europe. Only Belgium formally transposed the Recommendation into legislation[5] (Gustin, 2003; Lambert, 2002). Denmark already had similar rules before the Recommendation was enacted[6]. By the end of 2009, the situation will have changed dramatically, since all Member States will have to incorporate the same rules on liability into their national legislation. Since the Directive is based upon the principle of maximum harmonization, the Member States are in principle[78] not allowed to

[1] Directive 2007/64/EC of the European Parliament and the Council of 13 November 2007 on payment services in the internal market, amending Directives 97/7/EC,2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, *OJ L.* 319, 5 December 2007.

[2] http://www.pingping.be.

[3] Commission staff working document - Report on fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 - EU action plan /* SEC/2008/0511 final */

[4] Recommendation 97/489/EC of 30 July 1997 concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and the issuer, *OJ.L.* 208, 2 August 1997, 52.

[5] Act of 17 July 2002, Official Journal 17 August 2002: http://www.ejustice.just.fgov.be/wet/wet.htm.

[6] Payment Cards Act of 1984, replaced by the Act of certain payment instruments of 31 May 2000: http://www.forbrug.dk/fileadmin/Filer/FO_English/UK-betalingsmiddellov.pdf.

[8] However, in cases where the payer has neither acted fraudulently nor with intent failed to fulfill his obligations under article 56 (infra nr. 6), Member States may reduce the liability

incorporate more stringent provisions, offering a higher level of protection to the holder of an electronic payment instrument, into their national legislation.

In general, several types of fraudulent use need to be distinguished. First, the payer himself might act fraudulently. Secondly, the instrument might be counterfeited. Third, the instrument itself might get lost or stolen. Fourth, a third party might be able to intercept the credit card details and use these to make payments at a distance. In a situation like this, the card itself remains in the payer's possession.

Part 1. Fraudulent use of "traditional" electronic payment instruments

2. This part of the article only deals with the "traditional" electronic payment instruments, such as debit cards, credit cards, e-banking systems and electronic money instruments, such as Mondex (UK), Proton (Belgium) and the Geldkarte (Germany).

Chapter 1. Fraudulent use by the payer

3. In all legal systems the payer will bear the financial consequences of fraudulent use if he himself acted fraudulently (*fraus omnia corrumpit*). This situation occurs for example when the payer notifies loss or theft and then immediately after that withdraws money, or when the payer denies to have authorised a payment transaction, he initiated himself using his credit card details (card number and expiry date). In Belgium, the payer acting fraudulently can also be sanctioned by penal law (article 504 quater Penal Code) (Roger France, 2004).

Although this rule is clear from the legal point of view, it will not always be possible for the payment service provider to prove that the payer acted fraudulently.

Chapter 2. Counterfeited instrument

4. Losses which result from the use of a forged instrument have to be borne by the payment service provider. This is logical since it is up to the payment service provider to ensure that instruments cannot be counterfeited, or if he is not capable of doing so, to bear the financial consequences resulting from it[9]. Such rule can be seen as an application of the "Sphärentheory", which implies that the risk must be borne by the person who is best placed to avoid that the risk is realised (Ulmer, 1938; Thevenoz, 1990). Although the Directive does not contain an explicit rule on liability in case an instrument is counterfeited, this solution can also be derived from recital 32 of the Directive, which states that the Directive should be without prejudice to the payment service providers' responsibility for technical security of their own products.

---

referred to in article 60 of the Directive, taking into account, in particular, the nature of the personalized security features of the payment instrument and the circumstances under which it was lost, stolen or misappropriated.

[9] In this context it is interesting to emphasize that it is pretty simple to counterfeit payment instruments that are identified on the basis of a magnetic stripe, since the magnetic stripe can be copied easily. Smart cards on the other hand are very hard to copy, and therefore offer more security.

Chapter 3. Lost or stolen instruments

5. Article 53.3 of the Directive determines that the basic rules on liability in case of fraudulent use of electronic payment instruments also apply to electronic money instruments. Nevertheless it is useful to distinguish between these two categories of instruments, since the Directive contains a very important exception to this basic rule, where it states that the basic liability scheme does not apply to electronic money instruments when the payment service provider, who was notified about the loss or theft of the electronic money instrument, is not able to freeze the payment account or block the payment instrument.

With regard to the ability to freeze the further use of the payment instrument, it is necessary to make a distinction between transactions where the instrument is used to pay for goods, and services and transactions where new value is loaded upon the instrument. With regard to the latter, the payment service provider should always be able to prevent these, because a connection is made to the payer's account. The exception therefore only applies to payments executed with the instrument.

§1 Electronic payment instruments, excluding payments made with an electronic money instrument

6. According to the European Directive a distinction must be made between transactions that have taken place before notification of loss or theft of the instrument and transactions that have taken place after notification of loss or theft. With regard to the latter, it will be the payment service provider who will be held liable; with regard to the former, the payer bears the risk, which however is limited to € 150 except in case of extreme negligence.

A. Transactions taking place after notification

7. The payment service provider bears the financial consequences of the use of the lost or stolen instrument once notification has taken place (article 61.4). Whether the payment service provider is actually able to prevent further use of the instrument is irrelevant. Also, it is irrelevant whether the payer acted grossly negligent. Therefore, extreme negligence doesn't play a role at all with regard to transactions that have taken place after notification.

This is logical. Payment service providers must bear the risk of fraudulent transactions after notification, since they are best placed to prevent further fraudulent transactions by blocking the instrument. This rule can once again be seen as an application of the "Sphärentheory" (Favre-Bulle, 1992).

8. Today, the contractual terms of some payment service providers determine that the payment service user whose payment card has been stolen, must file a complaint at the police station. The non-fulfilment of this obligation cannot under any circumstances exempt the payment service provider from liability for transactions that have taken place after notification (Caen 24 June 1993, *La Semaine Juridique Entreprise et Affaires* 1993, 349; Bouteiller, 2000). As soon as notification has been done the issuer must prevent further use of the instrument.

B. Appropriate means for notification

9. The payment service provider must ensure that appropriate means are available *at all times*, enabling the payment service user to notify the loss, theft or misappropriation of payment instruments (article 57). Therefore it must be possible to notify loss or theft seven days a

week, 24 hours a day. Although not explicitly determined, it is clear that the payment service user must have the possibility to notify the payment service provider by phone, as this usually is the fastest way to notify loss or theft and therefore the best way to prevent further transactions. Also, the payment service provider must provide the payment service user with the means to prove that he has made such notification (article 57).

The Directive contains a specific sanction in case the payment service provider does not fulfil its obligation to provide appropriate means to notify loss or theft (article 61.5). More specifically, in such situation the payment service user cannot be held liable for the financial consequences resulting from the use of the lost, stolen or misappropriated payment instrument, except if he acted fraudulently. So the payment service provider will be held liable for all transactions that have taken place, either before or after notification and whether or not the payment service user acted grossly negligent.

This sanction, which is also incorporated in the Belgian Act of 17 July 2002 on electronic payment instruments, is very severe. The payment service provider will not only be liable for those transactions that have taken place between the point in time where the payment service user tried to notify the payment service provider (but was not able to do so because no appropriate means for notification were available) and actual notification. Moreover, he will be liable for all transactions that have taken place, so even for those transactions that have taken place before the payment service user tried to notify the payment service provider.

C. Transactions taking place before notification

10. The payer bears the losses resulting from the use of the lost, stolen or misappropriated payment instrument, occurring before he has fulfilled his obligation to notify the payment service provider. However the liability of the payer is limited to € 150, unless the user has acted fraudulently *or has failed to meet the obligations imposed on him by article 56 of the Directive with intent or gross negligence*, in which situation he is liable without upper limit (article 61.2).

It seems that this rule cannot be seen as an application of the "Sphärentheory". According to this theory, the payer should be held liable for transactions that have taken place before notification, since the payer is best placed to avoid fraudulent transactions as long as notification has not taken place (Bieber, 1986). So in comparison with the "Sphärentheory", the Directive contains a liability regime which is more user friendly, unless one would argue that the payment service provider is actually best placed to avoid fraudulent transactions because the payment service provider is the only one who can develop techniques which eliminate fraud (such as biometrics).

11. As the payer is liable without any limitation in case of gross negligence it is important to find out what constitutes gross negligence and who must prove its absence or its existence. The concept of gross negligence is not defined in the Directive. Article 61.2 only indicates that the payer is liable without limitation *in case of gross negligence with regard to his obligations under article 56*. More specifically it concerns the obligation of the payer 1) to use the payment instrument in accordance with the terms governing the issuing and use of the instrument; 2) to take all reasonable steps to keep safe the security features of the payment instrument; and 3) to notify the payment service provider or the entity specified by the latter, without undue delay of the loss, theft or misappropriation of the payment instrument or of its unauthorised use.

Contrary to the Recommendation (article 6.1), the Directive does not determine that the payer is liable without upper limit as soon as he violates one of the obligations imposed by article

56. Under the Directive, such violation only leads to unlimited liability when the judge considers the violation to be a gross negligence. In Belgium, for example the Court of Appeal in Brussels decided that gross negligence requires something more than mere carelessness (Brussels 4 oktober 2005, *Droit bancaire et financier* 2006, 148).

12. In order to determine whether certain behaviour constitutes gross negligence, the judge has to take into account all relevant circumstances. The fact that the non-fulfilment of the obligation to take reasonable steps to keep the instrument safe may constitute gross negligence, gives the judge a great discretionary power. It illustrates that all kinds of behaviour can be considered gross negligence. In what follows, we will try to find out which behaviour could be regarded as gross negligence and whether payment service providers can define or fill in the concept of gross negligence in their general terms and conditions.

a) Recording the PIN

13. Contrary to the European Recommendation (article 5 (c)) and the Belgian Act of 17 July 2002 on Electronic Payment Instruments, the Directive does not explicitly determine that it is prohibited to record the personal identification number on the instrument (or on a document kept together with the instrument) in an easily recognisable form. However, this does not mean that the payer can record his PIN on the instrument. Indeed, article 56 determines that the payment service user must take all reasonable steps to keep the security features of the instrument safe and it is clear that this obligation prohibits that the PIN is written on the instrument.

More controversial is the question whether the PIN can be recorded on the instrument or on a note which is kept together with the instrument, in an encrypted form. For example, what to do if a card holder encrypts his personal code in a phone number? In Germany the court of Kassel decided that a card holder that incorporates his PIN in a phone number, written down on a paper in his wallet, acts extremely negligent (AG Kassel 16 November 1993, *Zeitschrift für Wirtschafts- und Bankrecht* 1994, 2110). In the Netherlands 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 (GCB 24 September 1994, *Tijdschrift voor consumentenrecht* 1995, 183). It is clear that the circumstances will determine the outcome.

In any case, I believe that payment service users should have the possibility to record their PIN, as long as they do not keep the document which mentions the PIN, in the same place as their payment instrument. Indeed, not everyone will be able to remember his PIN, especially since payment service providers ask their clients to use a different and not easily traceable (e.g. 1111 or anniversary date) PIN for every payment instrument.

b) Leaving the instrument in a place accessible to others

14. It is possible to argue that a payment service user acts grossly negligent with regard to the obligation to take all reasonable steps to keep the instrument safe, when he leaves the instrument in a place which is accessible to other, non related persons. This view seems to be accepted in Belgian jurisprudence. For instance, it has been decided that an old lady acted grossly negligent when she left her credit card in her hospital room while being examined (Juge de Paix Brussels 7 July 2006, *Droit bancaire et financier* 2007, 134. The judge was not prepared to take into account the stress of a hospitalisation, since the old lady had been clever enough to store her money (but not her credit card) in a safety box). In another case the judge

found that the card holder acted grossly negligent by leaving his payment card in a hotel room while going to breakfast, the room being accessible to the hotel staff (Commercial Court Brussels 27 November 2006, *Droit bancaire et financier* 2007, 137). On the other end, the payment service user does not act grossly negligent if the card is stored out of sight in a place which is locked. For example it has been decided in Belgium that a card holder does not act extremely negligent when he leaves his card in the glove compartment of his locked car (Brussels 13 september 2005, *Droit bancaire et financier* 2006, 145, note R. Steennot).

c) Late notification

15. Traditionally it is accepted that late notification constitutes gross negligence (OLG Hamm 17 March 1997, *C.R.* 1997, 339; LG Halle 27 October 2000, *Zeitschrift für Wirtschafts- und Bankrecht* 2001, 1298 (Germany); Lyon 26 June 1996, *Revue de Droit bancaire et bourse* 1997, 164 (France))[10]. Thus the payment service user must act promptly as soon as he finds out that his instrument is stolen, lost or misappropriated. As it is impossible to prove the actual knowledge of loss or theft of the instrument, it is sufficient that the payment service user *should have been* aware of loss or theft. For example, as soon as the payment service user has received his statements of account, mentioning the fraudulent transactions, he is or at least should have been aware of loss or theft.

In this context the question arises whether a card holder is obliged to permanently verify whether the instrument is missing. At least in Belgium, this is not the case. In one case the Court of Appeal in Brussels decided that a card holder does not act grossly negligent if he only finds out after one month that his card is missing (Brussels 27 May 2002, *Nieuw Juridisch Weekblad* 2003, 311; *Revue de droit commercial belge* 2004, 158). In another case the same Court argued that in case someone gives you back your wallet that has fallen out of your pocket, you do not need to verify immediately that your card is still present (Brussels 4 October 2005, *Droit bancaire et financier* 2006, 148).

16. It is important to stress that the payment service user, who notifies the issuer too late, is liable for all transactions that have taken place before notification and not only for those transactions that have taken place between the point in time where he should have notified the payment service provider and the moment actual notification has taken place. I find this rule too severe for the payment service user. 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 a gross negligence, leading to unlimited liability of the payment service user. Indeed, such regime is very disadvantageous for the payment service user as damages can be very high in case of a late notification. Second, even if one accepts that late notification constitutes gross negligence, the payment service user should only be liable without limitation for the transactions that have taken place after that point in time where he should have notified the payment service provider, either because he has become aware of loss or theft, or because he should have become aware of loss or theft of the instrument.

17. At this point, it is useful to compare the European regime with the rules incorporated in the United States Electronic Funds Transfer Act. First of all, it must be stressed that the concept of gross negligence does not play a role in this Act. The only thing that matters is the timeframe within which notification has taken place. More specifically, 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*, the consumer will be liable for unauthorised transfers only up to a value of 50

[10] KKO 1994:82, mentioned in the Study of the implementation of the Recommendation 97/489/EC, 14 (Report on Finland).

USD or the amount of the unauthorised transfer that occurred before notice to the financial institution (whichever is less). 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 loss or theft within sixty days of the transmittal of the periodic statement, on which the unauthorised transfers are recorded, he will be liable for all transactions that have taken place after this period of sixty days and before notification.

Contrary to what is the case in Europe, the mere fact that notification does not take place immediately after becoming aware of loss or theft does not lead to unlimited liability.

d) The role of the contractual terms

18. Many payment service providers define the concept of gross negligence in their general terms and conditions, in most cases by enumerating behaviour that must be regarded as gross negligence. The question arises whether the judge is bound by those terms. The answer to this question is clearly negative, since the rules on liability incorporated in the Directive are mandatory. If one would accept that payment service providers can freely determine which behaviour constitutes gross negligence they would have the possibility to avoid the application of the limitation of liability up to € 150 simply by describing the concept of gross negligence very broadly. Therefore, even if the contractual terms define gross negligence, it will be up to the judge to determine whether certain behaviour constitutes gross negligence or not. However, all of this does not mean that contractual terms relating to gross negligence are completely irrelevant. By describing in the contractual terms which behaviour entails certain risks, the payment service provider informs the payment service user about the existing risks. The judge will hold someone who is informed about the risks more easily liable than a person who was not informed, because the former is deemed to have more knowledge of those risks.

e) Distraction in a selfbanking area

19. Recently payment service providers in Belgium warned about fraud in selfbanking areas. What happens, is the following : the payment service users, especially elderly people are distracted when they end a transaction at a terminal in a selfbanking area. In doing so, the frauds try to steal the payment card when it comes out of the terminal. Once they have obtained the card, they say to the payment service user that an error probably occurred and the card can be retrieved by keying in the PIN once again. If the payment service user keys in the PIN and the fraud is able to see it, it becomes very easy to withdraw money with the stolen card. The question is of course whether in a situation like this, the payment service user has acted grossly negligent. We believe this is not the case, since gross negligence requires more than mere carelessness.

D. The burden of proof

20. The question arises who must prove that the transaction is (un)authorized and who must prove the absence or existence of gross negligence. On the one hand one could argue that the payment service provider should prove that the payer authorized the transaction and acted with gross negligence. But how could the payment service provider deliver this proof, for example if the payer denies he has authorized the transaction and denies that he has written his personal code on a paper in his wallet? On the other hand, how could the payer prove that he was not grossly negligent? After all, this supposes the proof of a negative fact.

21. Contrary to the Recommendation, article 59 of the Directive contains rules relating to the burden of proof. When a payer denies having authorised an executed payment transaction, the payment service provider must prove that the payment transaction was authenticated, accurately recorded, entered into accounts and not affected by technical breakdown or another deficiency (article 59.1). Therefore, it is up to the payment service provider to prove that the transaction was authenticated, for example to prove that the instrument and the PIN have been used. This rule however does not determine who has to prove that the transaction was (un)authorized and who bears the burden of proof with regard to the absence or existence of gross negligence. But in this context article 59.2 is relevant. It determines that the use of a payment instrument, recorded by the payment service provider is in itself *not necessarily sufficient* to prove either that the transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under article 56. *Not necessarily*, what does this mean?

Recital 33 states: *The evidence and degree of alleged negligence should be evaluated according to national law. Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered null and void*. This recital does not determine who bears the burden of proof. It only states that contractual changes to the burden of proof are not allowed if they are disadvantageous to the payer.

In an answer of 6 October 2008 to question 112 (FAQ)[11] the European Commission states: *In the case where the payment service user denies having authorized a transaction, the use of a PIN is not a sufficient proof: the PIN might have been caught at the same time as the card data in the case of a fraud*. This answer seems to indicate that the burden of proof with regard to the question whether or not a transaction is authorised, is imposed on the payment service provider. However in an answer to question 84, asking *how the payer's payment institution can verify that the payer has authorized this payment transaction*, the Commission states: *In case of card transactions, the payment service provider may check whether the payer has entered his PIN code or signed an authorization form.*

Taking into account both answers, it is not clear who, according to the European Commission, must bear the burden of proof with regard to the authorized or unauthorized character of the payment transaction. To me, it seems logical that in principle it is up to the payer to at least make it probable that he did not give his consent to the payment transaction. Indeed, in many cases, there are no other means available to the payment service provider to prove that the payer authorized the transaction (Henard, 2009). But, whenever possible the parties should collaborate! For example if the payment service provider films money withdrawals at automatic teller machines and the payer denies having authorized a transaction at an ATM, the payment service provider should use these images to find out whether or not the transactions has been authorized.

Furthermore, in case it has become clear that the transaction was unauthorized, these answers do not determine who must prove the absence or existence of gross negligence. Today, a presumption of gross negligence is used in several jurisdictions within the European Union (e.g. in Germany where the theory of the *Anscheinsbeweiß* is applied (BGH October 2004, http://www.jurpc.de/rechtspr/20040285.htm; OLG Celle 27 February 1985, *W.U.B.* 1985, 95; Spallino, 2001; Werner, 1997). The mere fact that a third person has been able to use the instrument protected by a personal identification number leads to the presumption that the

[11] http://ec.europa.eu/internal_market/payments/docs/framework/transposition/faq-2009_04_24_en.pdf.

holder has acted grossly 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 gross negligence. However this view is not shared in all countries. In the Belgian Act of 17 July 2002, the legislator explicitly prohibits the use of a presumption of extreme negligence (article 8). The mere fact that a third person was able to use the instrument cannot prove that the holder of the instrument has been negligent. So it is up to the issuer to provide elements that prove the existence of extreme negligence (Brussels 4 October 2005, *Droit bancaire et financier* 2006, 148).

We believe that it was not the European legislator's intention to completely prohibit the use of a presumption of gross negligence. If this would have been the intention, the Directive should have determined that the use of the PIN in itself is not sufficient (instead of not necessarily sufficient) to prove that the payer acted grossly negligent.

It is finally worth mentioning that the text of the proposal was not much clearer, where it stated that the payer had to provide factual information or elements which would allow the presumption that he could not have authorised the payment transaction and could not have acted with gross negligence or fraudulently.

22. Anyhow, the question arises whether it is justified to impose the burden of proof concerning the absence of gross negligence on the payer (Berkvens, 1997). First of all, it might be useful to make a distinction between the instruments used. Instruments such as debit cards and credit cards are far more sensitive to loss and theft than for example e-banking systems that make it possible to initiate credit transfers on the Internet. Moreover, fraud with e-banking systems is often committed by persons from the payer's direct environment. Taking into account these facts, it is probably justified to apply a presumption of gross negligence in case fraud with such instrument is committed.

Secondly it is probably justified to make a distinction between loss and theft of the instrument (Favre-Bulle, 1998). In case of loss it is hard to imagine a situation in which fraudulent use is possible without the payer acting grossly negligent. Therefore it is justified to impose the burden of proof on the payer. In case of theft on the contrary, there is a chance that the holder did not act grossly negligent - for example it is possible that the thief has spied on the payer before stealing the instrument - so that it is justified to impose the burden of proof on the payment service provider. However, in many situations it is impossible to determine whether the instrument has been lost or stolen. In a situation like that, it is preferable to impose the burden of proof on the provider. First the payment service provider is the party that is best placed to introduce technical solutions that further limit the risks of fraudulent use of electronic payment instruments by third parties. Secondly, and this is the most important argument, such solution avoids that the limitation of liability to € 150, which is the main feature of the liability system, becomes in many situations purely fictitious, which will be the case when a presumption of gross negligence is used.

§ 2 Payments made with an electronic money instrument

23. As already indicated, article 55.3 determines that the basic rules on liability in case of fraudulent use of electronic payment instruments also apply to electronic money instruments, except when the payment service provider, that was notified about loss or theft of the electronic money instrument, is not able to freeze the payment account or block the payment instrument. Since many electronic money instruments, such as proton, work off-line when payment is made, it is technologically impossible to prevent further payments. Therefore in

most cases the payment service user will bear the loss of the remaining value on the instrument.

However, in some situations the payment service provider will be in a position where he is technically able to freeze or prevent the further spending of the value stored on an electronic device, even if payments are made off-line. For example, if the payment service user has one payment card, serving as electronic money instrument and as debit card, and the holder has reported the loss or the theft of the card and the issuer was able to recover the card (e.g. because the thief tried to use the card after notification at an ATM). In such situation the Directive obliges the payment service provider to refund the value stored on the electronic money instrument.

Chapter 4. Misappropriation of the payment instrument

24. Sometimes an instrument is used fraudulently, without the instrument being lost or stolen. This occurs for example when a third person was able to write down the credit card features and uses these detail to shop on the Internet (where the payment is made by communicating the credit card details). The Belgian Act of 2002 and the European Recommendation explicitly determine that the card holder cannot be held liable, not even if he acted grossly negligent, if the fraud occurs without the physical presentation and electronic identification of the instrument, which is the case if a third person only communicates the credit card number and expiry date.

The Directive does not contain an explicit rule which determines that the holder cannot be held liable in case the instrument is used fraudulently without physical presentation and electronic identification of the instrument. Does this mean that the basic liability regime also will have to apply for example to payments effectuated on the basis of the number and expiry date of the credit card (Henard, 2009; This author believes that the basic liability scheme will apply)?

25. In answering this question one has to take into account article 61.1 of the Directive. This article makes clear that a distinction must be made between loss and theft of the instrument on the one hand and misappropriation on the other hand. In the latter case the payer can only be held liable (up to € 150) for transactions that have taken place before notification if he failed to keep his personalised security features safe. It is clear that the credit card number and expiry date are not personalised security features. But what happens in case of gross negligence of the card holder (e.g. the card holder left the credit card on the dashboard of his car, which was unlocked)? In case of gross negligence (article 61.2) the Directive does not distinguish between loss, theft and misappropriation. Article 61.2 applies to all unauthorised transactions.

Does this mean that the card holder will be held liable without any limitation for these types of ‘unsecure’ fraudulent transactions? I don’t think so. One has to take into account that the payer can only be held liable if the payment service provider can prove that the transaction has been authenticated (article 59). According to article 4.19, authentication means a procedure which allows the payment service provider to verify the use of a specific payment instrument, *including its personalized security features*. One can argue that the credit card number and its expiry date do not constitute personalized security features. If one accepts such reasoning, the card holder cannot be held liable if someone else has used his credit card details to pay for goods and services at a distance, since the payment service provider will not be able to prove that the transaction was authenticated.

Part 2. Fraudulent transactions with mobile payment instruments

Chapter 1. Scope of application of the Directive

26. Mobile payments, i.e. payments initiated using a mobile phone, are without any doubt payment transactions; so basically, these transactions fall under the scope of the European Payment Services Directive and the rules on liability incorporated in it. However, in determining the scope of application of the Directive, one must also take into account article 3 of the Directive regarding the transactions that are excluded from the Directive.

More specifically, the Directive does not apply to payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services (article 3.l). So, basically, there are two requirements:

1. the goods or services must be delivered through a telecommunication, digital or IT device (which is for example not the case if the mobile phone can be used to purchase soft drinks or food);
2. the telecommunication, digital or IT operator does not only act as an intermediary between the payment service user and the supplier of the goods and services. Therefore if the activity of the operator goes beyond a mere payment transaction, the Payment Services Directive is not applicable (see also recital 6).

The new mobile payment system pingping, which is introduced in Belgium, will certainly fall under the scope of application of the Payment Services Directive, since it will be possible to use the mobile phone to purchase low-value goods, such as soft drinks, sandwiches, etc.

Chapter 2. How does pingping work?

27. Before describing the applicability of the rules on liability mentioned above, it is useful to explain very briefly how pingping works.

Pingping makes it possible to use the mobile phone as an electronic money instrument, on which monetary value can be stored. First, the mobile phone can be used to pay for small amounts, simply by scanning the pingping tag, placed on the mobile phone[12]. Contrary to what happens in case of the use of Proton, the other Belgian electronic money instrument, which has taken the form of a smart card, payments take place contactless. In some cases, for example if the payer wants to buy a can at a vending machine, it is necessary to send an sms, i.e. a text message, with the vending machine number[13].

Of course, in order to be able to use the mobile phone as an electronic money instrument, monetary value must be loaded upon the phone (pingping account). This can be done in several ways: by a credit transfer to the operator of the system, by debit card and credit card. In case the uploading takes place with a debit card or credit card, a secure website needs to be used. When the debit card is used, the card holder must identify himself in the same way as to initiate payment transactions on his e-banking system (sometimes the card must be inserted in a terminal and a PIN keyed in, sometime a user's number and a PIN needs to be keyed in).

[12] http://www.youtube.com/watch?v=-Cese5GlA2M&feature=player_embedded
[13] http://www.youtube.com/watch?v=zBPpTWLcWI0&feature=player_embedded

When the credit card is used, sometimes the PIN is required; sometimes it is sufficient to key in the credit card's number, expiry date and verification code. Everything depends on the bank that issued the credit card.

Another way of mobile paying which is made possible by pingping is using sms to transfer money to another person, the only requirement being that that person has a valid Belgian telephone number. In order to initiate a transaction it is necessary to key in a PIN. More specifically, the text message's content is the following : "P (amount) (mobile phone number beneficiary) thank you (Pin)"[14]. If the beneficiary of the payment transaction hasn't got a pingping account yet, he will receive an sms notifying him he has received an amount and asking him to open an account. Once the account has been opened, the amount received can immediately be spent by the beneficiary.

Chapter 3. Liability in case of fraudulent use of the mobile phone, serving as a payment instrument

§ 1 Types of fraud

28. In case someone loses his mobile phone or his mobile phone is stolen, further use of the instrument can be prevented by notifying loss or theft to Tunz (the company issuing pingping). Notification can only be done by sending an sms, which implies notification can only take place if you are allowed to use the mobile phone of another person. Once loss or theft are notified, it is no longer possible to perform payment transactions with the mobile phone.

Before notification a third party will be able to execute at least some transactions. Indeed, not all transactions require that a PIN is used. For those transactions where a PIN is necessary, the third party will only be able to use the mobile phone as a payment instrument if he has been able to find out the PIN as well. Two remarks must be made here. First at the moment, when opening an account at Tunz, the PIN is sent by sms. If this sms is not deleted (the general terms require the payer to delete the sms with the PIN immediately) the third party will be able to find out the PIN very easily. Secondly, is it always possible to apply for a new PIN by sms. In a case like that a new PIN will be sent after 4 hours. According to Tunz, this period of time should avoid that the new PIN is received before notification of loss or theft of the mobile phone. I find this is a rather short period of time.

29. Another type of fraud occurs when a person uses someone else's credit card or debit card to load monetary value upon his mobile phone (not working on a postpaid basis, but on a prepaid and therefore anonymous basis (If the fraud has a subscription to use pingping, it will be easy to detect him)). Especially the use of credit cards creates risks, more specifically if it is possible to load value upon the pingping account by simply transmitting the credit card details. In other cases fraud with credit and debit cards is less likely since the thief will need the PIN of the card to initiate the transaction.

§ 2 Liability for fraudulent transactions

30. As indicated, the rules on liability incorporated in the Payment Services Directive apply to fraudulent mobile payments (at least if they do not fall under the exclusion of article 3.l of the Directive). This means that a distinction must be made between payment transactions in which the mobile phone serving as an electronic money instrument is used fraudulently and

[14] http://www.youtube.com/watch?v=BIqK9foFi7M&feature=player_embedded

other fraudulent transactions within the mobile payment system (e.g. when the credit card number of another person is used to load money on the pingping account).

A. Fraudulent payment transactions with the mobile phone itself

31. As already indicated, article 55.3 determines that the basic rules on liability in case of fraudulent use of electronic payment instruments, also apply to electronic money instruments, except when the payment service provider that was notified about the loss or theft of the electronic money instrument, is not able to freeze the payment account or block the payment instrument. In case mobile phones are used as electronic money instruments, it is possible to prevent further fraudulent payment transactions, since the phone itself can be blocked. Therefore, the payment service provider will be liable for all transactions that have taken place after notification, even if the payment service user acted grossly negligent. The payment service user will be liable for transactions that have taken place before notification, but liability will be limited to € 150, unless when the payer acted grossly negligent. Looking at the pingping payment system today, we can see that the possibility to load value upon the instrument is limited to € 150, which implies that as long as notification has not taken place, the payment service user will *de facto* bear the losses of all fraudulent transactions.

B. Other fraudulent transactions within the pingping system

32. In case monetary value is loaded upon the mobile phone, using the payment instrument or the payment instruments details of another person, the rules applicable to that instrument will apply. More specifically, if the debit card of a third person is used, the rules on fraudulent use of a debit card will apply, meaning that once again a distinction must be made between transactions taking place before and after notification.

However, if fraud takes place by using the credit card features of a third person, we believe that the basic liability scheme does not apply, which implies that the credit card holder cannot be held liable for these transactions. As argued above, we believe that the credit card holder cannot be held liable, since the payment service provider will not be able to prove that these transactions were authenticated (supra nr. 24-25).

Conclusion

33. In the near future all Member States should have binding rules allocating liability. This is a good thing. However, not all problems are solved. More specifically, it is not clear who bears the burden of proof with regard to the authorized or unauthorized character of the payment transaction and who must prove the existence or absence of extreme negligence. As indicated, we believe that the general use of a presumption of extreme negligence is incompatible with the European legislator's objectives, since it would imply that the limitation of liability to € 150 for transactions taking place before notification becomes purely fictitious.

The rules on liability incorporated in the Payment Services Directive apply in principle to mobile payments. When applying the rules incorporated in the Directive to the newly introduced Belgian pingping system a distinction must be made between the use of the instrument as an electronic money instrument and fraudulent transactions which aim at uploading value. In this context it is especially worth to mention that the system makes it possible to prevent further payments by notifying the payment service provider. Once

notification has taken place the mobile phone cannot longer be used to pay. At this point there is an important difference between pingping and Proton. In the latter case, notification does not prevent the remaining value to be spent. However all of this does not mean that the use of pingping is without risks. Especially the use of credit cards to upload value creates risks, more specifically if value is loaded upon the pingping account by simply transmitting the credit card details.

References:

Berkvens, J. (1997) 'Elektronisch betalingsverkeer', *Computerrecht: tijdschrift voor informatica en recht*, pp. 264-265.

Bieber, K.D. (1986) 'Rechtsprobleme des ec-Geldautomatensystems', *Zeitschrift für Wirtschafts- und Bankrecht*, pp.12-13.

Bouteiller, P. (2000) 'Les relations juridiques entre banques et porteurs des cartes', *Banque*, No 70, pp. 31.

Favre-Bulle, X. (1992) Le droit communautaire de paiment électronique, Zürich: Schulthess, pp. 175-176.

Favre-Bulle, X. (1998) Les paiements transfrontières dans un espace financier européen, Basel: Helbing & Lichtenhahn.

Gustin, M. (2003) 'La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds', in C. Biquet-Mathieu (ed.), *Contrats à distance et protection des consommateurs*, Luik : CUP, pp. 183-227

Henard, G. (2009) 'L'exécution d'opérations de paiement non autorisées et l'inexecution ou l'exécution incorrecte d'opérations de paiement', *Droit bancaire et financier*, pp. 3-21.

Henard, G. (2009) 'L'exécution d'opérations de paiement non autorisées et l'inexecution ou l'exécution incorrecte d'opérations de paiement', *Droit bancaire et financier*, pp. 11.

Kierkegaard, S. (2007) 'Payments in the Internal Market and the New Legal Framework - EU Law: Harmonising the Regulatory Regime for Cross-Border Payment Services', *Computer Law & Security Report*, No. 2, pp. 177-187.

Lambert, T. (2002) 'La loi du 17 juillet 2002 relative aux opérations effectuées au moyen d'instruments de transfert électroniques de fonds', *Revue du droit commercial*, pp. 573-588.

Roger France, E. (2004) 'Transactions électroniques et crminalité informatique: quelle repression?', in *Aspects juridiques du paiement électronique*, Brussels: Kluwer, pp. 228-257.

Spallino, D. (2001) 'Rechtsfragen des Netzgeldes', *Zeitschrift für Wirtschafts- und Bankrecht*, pp. 231-241.

Thevenoz, L. (1990) Error and fraud in wholesale Funds Transfers. UCC Article 4A and the Uncitral Harmonization Process, Zürich: Schulthess, 120 p.

Ulmer, E. (1938) Das Recht der Wertpapiere, Stuttgart: Rothhammer.

Vanden Bosch, M. and Mathey, N. (2007) 'Le Marché unique des services de paiement en Europe', *Revue de droit bancaire et Financier*, pp. 59-70.

Werner, S. (1997) 'Anscheinsbeweis und Sicherheit des ec-PIN-Systems im Lichte der neueren Rechtsprechung', *Zeitschrift für Wirtschafts- und Bankrecht*, pp. 1516-1519.

Financial Law Institute

The **Financial Law Institute** is a research and teaching unit within the Law School of the University of Ghent, Belgium. The research activities undertaken within the Institute focus on various issues of company and financial law, including private and public law of banking, capital markets regulation, company law and corporate governance.

The **Working Paper Series**, launched in 1999, aims at promoting the dissemination of the research output of the Financial Law Institute's researchers to the broader academic community. The use and further distribution of the Working Papers is allowed for scientific purposes only. Working papers are published in their original language (Dutch, French, English or German) and are provisional.

More information about the Financial Law Institute and a full list of working papers are available at:
http://www.law.UGent.be/fli