CASE TRANSLATION: **SLOVAKIA**

Case citation:
Decision of the County Court Trenčín dated 19 June 2013, file ref. no. 17Co/213/2012

Name and level of the court:
Krajský súd Trenčín (County Court Trenčín)

Reference No:
17Co/213/2012

Identification number of the case file:
3111215045

Date of issue:
19 June 2013

ECLI:
ECLI SK: KSTN: 2013: 3111215045.1

Members of the court:
presiding judge, JUDr. Emília Zimová and judges JUDr. Gabriela Janáková and JUDr. Erika Zajacová

Areas of law:
civil law – other

The nature of the decision:
Confirmatory

Slovakia; online banking; customer mandate; theft by unknown third party; thief masquerading as a bank employee; false banking web site; anti virus software; negligence by a customer

JUDGMENT IN THE NAME OF THE SLOVAK REPUBLIC

A panel of the Regional Court in Trenčín, consisting of presiding judge, JUDr. Emília Zimová and judges JUDr. Gabriela Janáková and JUDr. Erika Zajacová in the case of the respondent U.. A. I., residing at J., K. XXXX/XB a citizen of the Slovak Republic, legally represented by O.. O. P., W seated in J., E.. S.. W. XX/XX against the appellant: Všeobecná úverová banka, a.s., with headquarters at I., A. E. X, U.: XX XXX XXX, regarding the payment of €3,485.60 euros, with interest, regarding the appellant's appeal against the judgment of the District Court Trenčín dated 8 March 2012, no. 21C/1432011-109,

has decided:

The judgment of the district court is hereby upheld.

The appellant is obliged to pay the respondent the court costs of the appeal proceedings consisting of costs of legal representation in the amount of €166.51, within three days from the effective date of this judgment, to O.. O. P., W..

Reasoning:

In the contested judgement, the district court ordered the appellant to pay the respondent €3,485.60 with interest of 9.25% per annum from 07.01.2011 until the date of payment, as well as reimbursement of the court costs consisting of payment of court fees in the amount of €209 and of the costs of legal representation in the amount of €665.94, within three days of the effective date of the judgment. Its decision was justified by a description of the facts, which showed that the respondent notified the appellant in writing on 01.02.2011 of the fact that on 05.12.2010, a sum of €3,000 had been deducted from their current account. The investigation found that the computer which the respondent had been using to log in to the internet banking site was infected by a computer virus that could have infected the computer in a number of ways, but not via the VÚB web site. After infection of the computer, the virus activated and generated a web page in the internet browser attempting to replicate the design of VÚB's internet banking site. The purpose of this fraudulent site was, by means of deception, to elicit sensitive authentication data and then send such to an unknown perpetrator. In this case, there was inadequate computer security against a malicious computer virus and the respondent thus voluntarily entrusted authentication data to an unknown thief. The thief, using this authentication data, later signed in to the internet banking site and executed a one-off payment. He then contacted the respondent, introduced himself as an employee of the bank, and informed the respondent that the bank had detected an attempt to execute a suspicious transaction and that to cancel this it was necessary to provide authentication using a position on the GRID card. The respondent provided the authorization element – the requested position on the GRID card, which was in fact used by the perpetrator to authorize the execution of the payment. The respondent confirmed that on the Sunday a person, claiming to be a bank

employee, communicated to him that suspicious operations made by a credit card were taking place on his account. On the same day, that person repeatedly called him and repeatedly stated that suspicious movements were taking place on his account and in order to block the credit card, the individual requested an authentication code by means of an SMS message. This code was provided by the respondent, and on the next day, 06.12.2010, he filed a complaint with the bank. Among other things, the appellant reasoned that the claim that the respondent had not sufficiently secured his computer using a sufficient authorized program, had not been proven by the respondent. It is not possible to consider that the respondent was negligent if he provides confidential data to a person that informs him, when on holiday, that suspicious transactions are taking place on his account. A typical client of the bank with average computer skills may not have sufficient expertise to recognize that there is a virus which is responsible for generating a fictitious internet banking site, or to know in detail the working procedures of the bank. The respondent did not give consent to the execution of the payment transactions in dispute and therefore the payment transactions cannot be considered authorized. On the earliest possible date, 06.12.2010, the respondent personally filed a complaint regarding the movements on the account to which he had not given consent. Moreover, the appellant themself confirmed that the unauthorized credit card transactions were effected in the period from 06.12.2010 to 15.12.2010, i.e. after the complaint had been brought.

The appellant filed an appeal against the judgement within the statutory period and proposed its cancellation and the return of the case to the District Court for further proceedings, or it's alteration so that the claim could be dismissed in its entirety. The grounds for appeal were under section 205 para. 2 letters a), b), d) and f) of the Civil Procedure Code (hereinafter the CPC). The decision of the Court of First Instance was appealed on the grounds that it was not convincing and did not meet the conditions which the legislator set out in section 157 para. 2 of the CPC and did not fulfil the requirements for verifiability and persuasiveness of judicial decisions. The appellant pointed out that the Court of First Instance limited the facts of the case to the respondent's description of the facts that the appellant had confirmed. Attention was not paid to the issue of computer security, and it was stated that the bank had failed to show that the respondent had not secured his computer. From the perspective of logic, it is difficult to imagine proving that adequate security was lacking, however it is simple to demonstrate that the computer had been secured. The Court of First Instance ignored the claims of the bank regarding instructions displayed to each customer concerning the safe use of internet banking as published by the appellant on the login page to internet banking since 2008. With each login, the respondent had thus the opportunity to carefully go through the information presented, in particular that containing a strong emphasis that customers should not respond to e-mails or telephone calls, in which anyone, including persons posing as bank employees would ask the customer to provide personal information, account numbers and balances or obtain access or authentication data. Such a notice for customers is formulated very simply and clearly, and also includes demonstrations and examples of similar attacks. The appellant pointed out that the court did not specify the term 'typical customer of the bank' and did not set out the reasoning to conclude that the respondent fell into this category and why the court considered that the typical bank customer does not need to take the opportunity to read the warnings on the internet banking login page . The appellant said that in addition to warnings on the login page, the bank emphasises the need for increased security in its general terms for deposit products and warns customers against the disclosure of authentication and security features to strangers. Since the respondent did not identify the person who, during a telephone call, they revealed the confidential information to, he would designate this person as a person unknown to the respondent. The appellant considers that it is necessary to clarify the action or inaction of the respondent to assess and question whether their behaviour could be assessed as negligent or not. The evaluation of the evidence should reflect the facts of the case and should be reviewable. The court did not address the bank's evidence, although the requirement set forth in the CPC is clear in that the court has to state in its decision regarding what evidence was examined and why. The appellant expressed disagreement with the conclusion of the Court of First Instance in that the payment transaction should be regarded as an unauthorized payment transaction. The appellant pointed to section 12 para 2 of Act no. 429/2009 Coll. (Correctly 492/2009 Coll.) under which the customer shall bear all the losses relating to any unauthorized

payment transactions if they were caused by his fraudulent conduct, wilful failure to fulfil one or more obligations under section 26 of the Act or failure to fulfil one or more obligations under section 26 of the Act due to their gross negligence. The obligations of the payment services user when using a payment instrument are listed in the cited statutory provision under letters a) to c). The appellant expressed the belief that the communication of security features to a person unknown to the respondent may be regarded as a breach of the normal precautions and thus gross negligence on the part of the respondent.

In the context of the provisions of section 25 of Act no. 429/2009 Coll., the payment services provider shall not be liable for breach of obligations in connection with the provision of payment services under the Payment Services Act where they prove that the breach was caused by circumstances that excluded liability or according to special regulation which states that the force majeure circumstances as defined in § 374 of the Commercial Code as obstacles that occurred independently of the will of the obliged party, and prevented it from fulfilling its obligations unless it can be reasonably assumed that the obliged party could avert or overcome this obstacle or its consequences and further, it had predicted such an obstacle at the time of formation of the obligation. He expressed the view that the appellant did not breach any obligation under the contract with the respondent in connection with the terms and conditions, nor did they omit to perform any obligation and therefore the bank cannot be fairly required to predict that at the time of the conclusion of the contract the respondent would, despite the bank's warnings , recklessly entrust confidential data to a person unknown to them, but on the contrary, with regard to the circumstances it could be stated that the respondent failed to take the necessary measures to avoid the damage and at the same time neglected the general obligation towards prevention. To conclude, the appellant pointed out that the respondent had filed a criminal complaint in the matter, on the basis of which a prosecution was launched, but the appellant was not familiar with the various stages of the prosecution, and therefore had no knowledge of whether and to what extent the respondent applied for damages in the criminal proceedings. Nor have they knowledge of which statements the respondent had made there, which can also be important information for the decision-making of the civil court in civil court proceedings; in particular, whether the law enforcement agencies identified the perpetrator of the offence and whether the respondent was successful in applying for damages.

The respondent in the statement, which was filed via his lawyer, suggested the judgment of the district court be confirmed as factually correct. They expressed the view that the payer bears, according to section 12 para. 1 of Act no. 429/2009, losses of up to €100, which are related to any unauthorized payment transactions and result from the use of a lost or stolen payment instrument or from the misuse of a payment instrument by an unauthorized person due to the negligence of the payer regarding the safeguarding of the personalized security features according to section 26 letter c). From para. 3 of the aforementioned provision, it follows that the payer shall not bear any financial consequences resulting from the use of a lost, stolen or misappropriated payment instrument from the moment of the notification of such events under § 26 letter b), except for cases where they have acted fraudulently. From the provisions of section 25 of the AoPS, it follows that the payment services provider is not liable for a breach of duties while providing payment services under this Act, provided that they prove that the breach of duties was caused by circumstances excluding liability, or proceed according to a special regulation. The payment services user, according to section 26 letter b), when using a payment instrument, is obliged to notify the payment services provider or a person authorized by the payment services provider without undue delay of loss, theft, misuse or unauthorized use of the payment instrument. In this case, a deduction of funds from the account of the respondent, as a user of payment services maintained by the appellant as a payment services provider, occurred on the basis of an unauthorized payment transaction, because the respondent never gave consent for the execution of the payment transaction by the appellant, which was carried out by the appellant nevertheless. The potential abuse of the technical means of the respondent, nor the potential eliciting of authentication data from the respondent by an unknown person cannot be considered as the provision of consent. Even if these facts would be proven, which would be up to the appellant to do, the respondent would only be negligent, and there would only be a misuse of the payment instrument by an unauthorized person due to the negligence of the respondent as the payer in terms of safeguarding the

personalized security features. To assess the legal claim for the damages in question it is therefore necessary to apply the provisions of section 12 para. 1 of the AoPS, under which the respondent is entitled to the refund of the full amount debited from his account without his warrant and knowledge, after a reduction of €100. The respondent has also shown, by documentary evidence, that the payment transactions which the respondent did not order, nor give consent to, were subject to his complaint filed on 06.12.2010 at a branch of the appellant in Trenčín, whereas further documentary evidence shows that the appellant himself confirmed that, in connection with unauthorized transactions made by the respondent's credit card, the appellant has on record international as well as domestic transactions charged to the account of the respondent between the days of 06.12.2010 and 15.12.2010, ergo in a substantial part after the date of notification carried out by the respondent in accordance with section 26 letter b) of this Act, and therefore in this way the appellant's procedure was wrong. The respondent considered as legally irrelevant the appellant's reference to the provisions of the appellant´s general terms and conditions regarding deposit products, because these cannot contradict the law, and even if this was the case, they cannot be applied when assessing the respondent's claim for damages to the extent in which they are inconsistent with the law. The damage incurred by the deduction of funds from the respondent's account without either their mandate or knowledge occurred in December 2010, whereas Act no. 492/2009 Coll., from which the respondent derives his claim, entered into force on 01.12.2009, and therefore the respondent's claim was to be judged under this legislation. Similarly, there is no legal significance in this case regarding the provisions of section 374 and section 384 para. 1 of the Commercial Code and the provisions of section 415 of the Civil Code. As for the criminal complaint filed by the respondent, the criminal procedure did not result in any findings significant for the assessment of the case, and the respondent was not able to claim damages.

The Regional Court considered the case under the provision of section 212 para. 1 of the CPC and found that the judgment of the District Court must be upheld under section 219 para. 1, CPC because the statement is as a matter of fact correct. This was decided without a hearing, according to a provision of section 214 para. 2 of the CPC according to which it is not necessary to order a hearing in front of the appeals court.

Judgment or an order terminating the main proceedings may, under the provisions of section 205 para. 2 of the CPC, only be justified by the circumstances referred to in letters a) to f) in the cited legal provisions.

The appellant invoked in his grounds of appeal under section 205 para. 2 letter a), CPC (issues referred to in section 221 para. 1 have occurred in the proceedings), followed by point b) (the procedure has a second other defect which could result in an incorrect decision in the case), d) (the Court of First Instance came to the wrong conclusions based on the examined evidence), f) (the decision of the Court of First Instance is based on a faulty legal assessment of the case).

The appellant in his appeal, however, did not specify any defects listed in section 221 para. 1, CPC or any other defects that could have resulted in an incorrect decision in the matter in this case, with the exception of a failure to comply with the requirements regarding the reasoning of the judgment under the provision of section 157 para. 2 of the CPC.

The formal requirements for judgments are governed by the provisions of section 157 paragraph 2, CPC so that in its reasoning the court has to note what the respondent claimed and for the reasons, the response of the appellant in the case, alternatively of other parties, briefly, clearly and concisely explain which facts were considered proven and which not, on what evidence was the decision based and what considerations led to the conclusion, why additional evidence was not examined and how the matter was assessed legally.

By examining the case, the Court of Appeal found that the reasoning of the judgment in question meets the requirements cited.

There is no doubt that the Court of First Instance stated in its reasoning what the respondent claimed and for the reasons, how the appellant responded and also explained the facts it considered proven and which not. It did so in the manner provided for in the cited statutory provision, i.e. briefly, clearly and concisely, stating that it did not consider proven the appellant's assertion that the respondent had not secured his computer using a sufficient authorized program, whereas it cannot be considered as negligent by the respondent if he provides

confidential data to a person that informs him, when on holiday, that suspicious transactions are taking place on his account. The situation where a party to the proceedings does not agree with the decision, and ergo the reasoning, cannot be considered as non-fulfilment of the formal requirements of the decision under section 157 para. 2 of the CPC and thus a violation of the right to judicial protection under article 46 para. 1 of the constitution.

The basis of the grounds for appeal under section 205 para. 2 letter d), CPC (the Court of First Instance came to the wrong conclusions based on the examined evidence) is mostly the wrong procedure of the Court of First Instance in assessing the results of the examination of evidence. As a result, the court takes into account facts that the evidence did not reveal or that were not submitted by the participants, or it ignores the facts that have been established by the evidence or arose from the parties' submissions. Errors of fact may as well be the result of logical contradictions in the evaluation of the evidence, with particular regard to the gravity, legality and accuracy of the acquired knowledge.

Where factual findings are not supported in the evidence, they shall be deemed to include the outcome of the evidence by the court, which does not correspond to procedures arising from the provision of section132, CPC. Under this provision, the court assesses evidence at its discretion, each piece of evidence separately and all of it in connection, having regard to all that came to light during the proceedings, including that which the parties had presented.

It would be possible to reprehend the Court of First Instance for incorrect assessment of the evidence, should it have taken into account facts that had not come to light from the examined evidence or the submissions of the parties, or otherwise during the proceedings, or alternatively, that it would not have noticed relevant facts that were proven by the performed examination of evidence, or had come to light during the proceedings, or alternatively because there were discrepancies regarding the evaluation of the evidence, or findings that emerged from the parties' submissions or came to light otherwise, mainly in terms of their severity, legality, truth or plausibility, or if the evaluation of evidence is in conflict with the provisions of sections 133 – 135 of the CPC. It is thus only possible to challenge a decision on the grounds of appeal under section 205 para. 2 letter d) CPC, with regards to the judicial consideration of evidence, nevertheless the inaccuracy can be understood solely from the way in which the court came to the decision.

In the present case, there is no doubt that from the respondent's account, which is maintained by the appellant, as a payment services provider, that there had been a cashless transaction made via internet banking, which had the effect of reducing the balance of funds in the account of the respondent by €3,000. By the very statement of the appellant, there is not any doubt that not even the appellant considered that the payment transactions had been carried out on the basis of an order by the respondent or with their knowledge. The subject of the proceedings, as well as of the appeal, is only the subsequent assessment of the appellant's responsibility for this financial transaction, with regard to the respondent's actions, which are also not in dispute (provision of information to a person who introduced themself as an employee of the appellant). In this case, therefore, not facts, but the legal conclusions are in dispute, making the application of the grounds for appeal under section 205 para. 2 letter b) of the CPC unjustified.

The grounds for appeal under section 205 para. 2 letter f), the CPC (the decision of the Court of First Instance is based on a faulty legal assessment of the case) can be successfully applied in the case of an erroneous application and interpretation of legal norms on the facts uncovered or the application of such a rule of law to the facts.

In the present case, the Court of First Instance proceeded according to the Act no. 492/2009 Coll, on payment services and on amendments to certain laws, which came into force on the 01.12.2009. The provisions of the above Act are also referred to by the appellant.

The object of the proceedings at the first instance, as well as on appeal, was the application of sections 11 and 12, in connection with sections 25 and 26 of the cited Act to the facts found in the case, as well as to the interpretation of these statutory provisions.

The duty of the payment services provider to return to the payer the amount of the unauthorized payment transaction is set out in section 11 para. 1 of Act no. 492/2009 Coll. This is a statutory obligation, and does not represent damages to which the payer is entitled under para. 2 of the cited statutory provision, and

which has not been applied in the present proceedings.

The obligations of the payer are outlined in section 12 of the above cited Act so that the payer, under para. 1, shall bear the loss relating to any unauthorized payment transactions up to €100.

Another duty, to bear all the losses relating to any unauthorized payment transactions, is provided for in para. 2 of the cited statutory provision and the appellant plead its application in their appeal. According to the cited statutory provision the payer shall bear all the losses relating to any unauthorized payment transactions, i.e. they are not entitled to reimbursement pursuant to section 11 of the Act, as long as the conditions specified therein are fulfilled. These are mainly actions of deception by the payer, which in this case was not even alleged by the appellant, just as intentional failure to meet one or more obligations under section 26.

The contents of the appeal show that the appellant seeks an application of the provisions of section 12 para. 2 of Act no. 492/2009 Coll., resulting in the situation that the respondent, as the payer, is to bear the losses associated with the unauthorized payment transaction, because it was caused by non-fulfilment of one or more obligations under section 26 as a result of their gross negligence.

According to section 26 of the cited Act, payment services users using a payment instrument are required to:

a) use the payment instrument in accordance with the conditions governing the issuing and use of this payment instrument,

b) inform the payment services provider or a person authorized by the payment services provider without undue delay of any loss, theft, misuse or unauthorized use of a payment instrument,

c) after obtaining or receiving the payment instrument, to take all reasonable steps to ensure the safeguarding of personalized security features of the payment instrument.

In the present case, it is without doubt that the respondent, as a payment services user, has met his obligation under the provision of section 26 letter b) in that he promptly notified the appellant of the unauthorized use of the payment instrument.

The appellant considers that the circumstances exclude their obligation because of the fact that the respondent, in connection with executing the payment transaction in question, gave his identification data to a person who introduced themself as an employee of the appellant. This conclusion results from the provision in section 12 para. 2, under section 11 para. 1 of Act no. 492/2009 Coll. However he himself submits that such behaviour of the respondent may be regarded as a breach of usual care.

If the Court of First Instance did not consider this conduct a gross breach of the obligations arising from the provisions of section 26 letter a) (to use the payment instrument in accordance with the conditions governing the issuing and use of this payment instrument) and thus a failure to meet a user's obligations due to gross negligence, the Court of Appeal identifies itself with this conclusion and thus considers the interpretation and application of the provision of section 12, significant for the legal assessment of the case, and as correct.

The County Court therefore upholds the judgment of the District Court.

The appeal was thus successful for the respondent who is, under provision of section 224 para. 1 of the CPC in connection with section 142 para. 1 of the CPC, entitled to reimbursement of the costs of the appeals proceedings, consisting of remuneration for one act of legal service for the response to the appeal in the amount of €131.13, pursuant to section 10 para. 1 of the decree no. 655/2004 Coll. + €7,63 flat rate + 20% VAT, totalling to €166.51.

The decision was taken by the panel of the County Court unanimously.

Instruction:

This judgment cannot be appealed.