CASE TRANSLATION: **SLOVAKIA**

Case citation:
Decision of the District Court Trenčín dated 8 March 2012, file ref. no. 21C/143/2011

Name and level of the court:
Okresný súd Trenčín (District Court Trenčín)

Reference No:
21C/143/2011

Identification number of the case file:
3111215045

Date of issue:
8 March 2012

ECLI:
ECLI SK:OSTN:2012:3111215045.4

Members of the court:
JUDr. Tatiana Porubänová

Lawyer for the plaintiff:
JUDr. Ján Legerský

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

JUDGMENT IN THE NAME OF THE SLOVAK REPUBLIC

The District Court Trenčín, presided over by a single judge Mgr. Tatianou Porubänová in the case of the plaintiff U.. A. I., residing at J., K. XXXX/XB a citizen of the Slovak Republic, legally represented by JUDr. Ján Legerský, an attorney seated in Trenčín, Nám. sv. Anny 15/25, against the defendant Všeobecná úverová banka headquartered in Bratislava, Mlynské Nivy 1, IČO 31320155, regarding the payment of €3,485.60, with interest,

has decided:

The defendant is obliged to pay the plaintiff €3,485.60 with interest of 9.25% per annum from 07.01.2011 until payment, within three days from the effective date of this judgment.

The defendant is obliged to pay to the court costs consisting of the court fee in the amount of €209 and the costs of legal representation in the amount of €665.94, within three days from the effective date of this judgment to JUDr. Ján Legerský.

Reasoning:

The plaintiff requested the court to order the defendant to pay them €3,485.60 with interest. He submitted that as the owner of the account and a customer, he concluded a contract regarding the provision of a current account and of 'flexiaccount' products and services with the defendant as the bank (hereinafter 'Contract') dated 01.08.2005, under which the defendant established in favour of the plaintiff a current account no. XXXXXXXXXX/XXXX (hereinafter 'Account') and provided him with, together with this account, a new Standard PK MasterCard credit card and set up an internet banking service for this account. The plaintiff, as the account holder, discovered that cashless money transactions were made, both via internet banking and also by credit card, which had the effect of reducing the balance of funds in the plaintiff's account. The cash operations were carried out without the knowledge or instruction of the plaintiff. The plaintiff reported the unauthorized withdrawals to the defendant immediately he became aware of the withdrawals, by means of a 'call center' that is in continuous operation and made available to clients of the defendant, whereby he also immediately lodged a complaint regarding these transactions affecting his account. On 06.12.2010, the plaintiff then went to a branch of the defendant located in Trenčín, Mierové námestie 37 to file a complaint in relation to transactions on his account that were made on 05.12.2010 and cleared on 06.12.2010, amounting to a total of €3,150. At the same time, the plaintiff on the same day and in the same place, in accordance with paragraph 7.4.1) and paragraph 7.5.1) of the General Terms and Conditions (hereinafter 'GTC') asked the defendant to cancel the freezing of funds held in his account in the amount of €2,382.60,[1] and the reason for this, as recorded in the

[1] The only issue to be resolved in this translation is 'freezing of the account' against 'cancellation of the withdrawal of the funds'. We are aware of the meaning 'freezing' with respect to an account, especially within AML regulation. Probably neither of the translations is suitable. The word used comes from Latin: *vinculum*.

notice of complaint, was that the plaintiff was contacted by the bank and informed about the misuse of the card. The card was, however, not stolen from the plaintiff nor lost, and the transaction carried out on the account by the credit card could only have been realized as a result of the misuse of data and unlawful conduct by a third party. The defendant did not respond in any way to the plaintiff's complaint until too late, according to the time limit for the complaint as outlined in the GTC, and informed the plaintiff with regard to the complaint regarding the cashless money transactions made via internet banking, that these were said to have been realized as a result of the careless actions of the plaintiff himself, in that he gave away an element of authorization via telephone to an unknown third party – a position on the GRID card, which is used for the authorization by an authorized person during the execution of credit operations through the service. On the basis of this, a misuse of the authorization element took place by way of entering it into a web site that imitated the defendant's internet banking web site, and was computer generated on the plaintiff's computer because his computer was affected by computer viruses. Based on these facts, the defendant stated that the plaintiff's complaint was deemed unfounded and the plaintiff was advised to contact the law enforcement authorities, to whom the defendant promised to provide full cooperation. In relation to the claimed monetary operations made on the account of the plaintiff through his credit card, the defendant stated that in relation to the unauthorized transactions made via the plaintiff's credit card, international and domestic transactions were on record, which were charged to the account of the plaintiff between 06.12.2010 and 15.12.2010. International transactions in the amount of €1,121.41 would be be refunded to the plaintiff's current account and with regard to the domestic transactions, the defendant would wait for the bank's statement, as well as statements from the affected merchants, and after receiving those statements the defendant would inform the plaintiff immediately. Since the plaintiff considered the defendant's progress in dealing with his claim entirely inadequate and partly inconsistent with the facts of the case, the plaintiff requested a re-examination of his complaints, again to no avail. The defendant maintained the opinion that regarding the banking transactions in dispute there was no wrongdoing by the bank. The plaintiff specified that up to that point, on the basis of his two complaints, only a part of the sum withdrawn without authorization from the account, in the amount of €1,947, had been reimbursed – a sum of €1,932.41 was reimbursed in January 2011 and a sum of €14.59 in March 2011.

On 14.10.2011 the court issued a payment order on the matter, no. 21C/143/2011-36, in which it fully upheld the claim.

The defendant filed a defence against this decision within the statutory period. They proposed the dismissal of the claims, and maintained their arguments as set out in their previous communications with the plaintiff.

The court examined the evidence by questioning the plaintiff, taking note of the essential content of the documentary evidence submitted by the plaintiff and found the facts of the case to be as follows:

On 01.08.25005 the parties entered into a contract regarding the provision of a current account and of 'flexiaccount' products and services, under which the defendant established in favour of the plaintiff a current account no. XXXXXXXXXX/XXXX.

On 06.12.2010, the plaintiff filed a written complaint to the defendant on the grounds that during December 2010 several transfers of funds occurred on his account without his knowledge or instructions.

On 01.02.2011, the defendant notified the plaintiff in writing that on 05.12.2001 a sum of €3,000 had been debited from the plaintiff's current account. During

Unfortunately, we cannot be certain that the translation is totally accurate, since we do not have access to the case file (it is also possible that the judge did not use the term properly).
One possible interpretation is that the amount of EUR 2,382.60 in the respective account had been blocked against any transaction before the fraud took place during some kind of arrangement made by the account holder. This is quite a common arrangement when the parties agree that the bank will not pay out certain funds unless certain event occurs and if so, then to a particular person. It is very similar to an escrow account but the difference is that an escrow is tripartite agreement – however, in case of the blockage of the payment, there two counterparties who agree so, and one of the parties subsequently instructs its own bank to block a payment from its own account. Therefore, during his visit, the account holder not only notified the bank of unauthorized transactions, but also wanted to cancel the blockage of payment. This interpretation fits the meaning of 'vinculum' as it is usually used, however, it does not fit into the context of the case.
Another possible interpretation, and another reason for using the words 'frozen account' is that once an authorized transaction is reported to a bank, the bank automatically freezes the account so that it prevents any other fraud attempts until a new GRID is generated (i.e. a new card is issued) and/or new access to internet bank is provided (new password etc.). Hence, it could happen that the account was frozen upon the call of the account holder to the bank when he notified an unauthorized transaction, and the next day the account holder asked that the account be unfrozen regarding the remaining funds. Although this would give more sense, it would indicate improper use of the word *vinculum*.

the investigation into the matter they found out that the computer from which the plaintiff viewed the internet banking web site was infected by a computer virus, which could have infected the computer by a number of ways, but probably not via VÚB's internet banking site. After the computer was infected, the virus activated and generated a web page in the internet browser attempting to emulate the design of VÚB's internet banking site. The purpose of this fraudulent site was, by using means of deception, to elicit sensitive authentication data and then send this to an unknown perpetrator. In this case, there was inadequate computer security against a malicious computer virus and the plaintiff thus voluntarily entrusted authentication data to an unknown fraudster. The fraudster, using this authentication data, later signed in to the internet banking site and executed a one-off payment. He then contacted the plaintiff, introduced himself as an employee of the bank and informed the plaintiff that the bank had registered an attempt to execute a suspicious transaction and that to cancel this it would be necessary to authenticate the cancellation by using a position on the GRID card. The plaintiff provided the authorization element – the requested position on the GRID card, which was in fact used by the perpetrator to authorize the payment being executed. The defendant further stated that more transactions were made through the plaintiff's credit card, both international and domestic, in the days between 06. – 15.12.2010. The defendant further stated that the amount of €1,121.41 from the international transactions would be refunded to the plaintiff's current account, and the domestic transactions would be subject to further investigation.

In a further written submission, the defendant confirmed that payments in a total amount of €5,532.60 were made from the plaintiff's account using the internet banking service and the credit card during December 2010. The defendant has repeatedly claimed that due to a computer virus, an unknown perpetrator tricked the plaintiff into providing authentication data required to log in to the internet banking service. The unknown perpetrator obtained an authorization code, required to confirm the payment, by telephone, claiming that he was a bank employee, and wanting to inform the plaintiff about suspicious transactions occurring on his account. To prevent these transactions, an SMS authorization code was needed. In this way, payments were made on 05.12.2010 and 06.12.2010 in the total amount of €3,150. By obtaining access to the internet banking service, the unknown perpetrator also obtained information about the plaintiff's credit card, due to which he executed multiple domestic and international payments, in a total amount of €1,932.41. The defendant also pointed out that all operations concerning the plaintiff's account were made on the basis of correct access data obtained by the unknown perpetrator as a result of the plaintiff's gross carelessness in failing to secure his computer, and moreover by the disclosure of the data needed to make the payments via telephone. The defendant submitted that due to such gross negligence by the plaintiff they cannot be held liable for loss incurred by the plaintiff.

The plaintiff 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 in his account. On the same day such a person repeatedly called him and repeatedly stated that suspicious movements were taking place on his account and in order to block the credit card they required an authentication code from an SMS message. This code was provided by the plaintiff and on the next day, 06.12.2010, he filed a complaint with the bank. The plaintiff claimed that he had not made any payments on 05.12.2010, and as for the credit card, he had the card on his person, he had not lost it or noticed that any unknown person would have had any opportunity to examine it.

From the provisions of section 2 para. 2 of Act no. 492/2009 coll., on Payment Services and on amendments to certain acts, which came into effect on 01.12.2009 (hereinafter 'AoPS') it follows that a payment transaction means a deposit of funds, withdrawal of funds or a transfer of funds upon instruction of the payer or the recipient, or by means of the recipient to the provider of payment services, executed within payment services under paragraph 1 letters a) to f).

From the provisions of section 2 para. 19 of the AoPS, it follows that a payment instrument, for the purposes of this Act, is a personalized device or set of procedures agreed upon between the payment service user and the payment services provider, in particular a credit card, internet banking or other payment applications derived from electronic banking.

From the provisions of section 8 para. 1 of the AoSP, it follows that if the payer has given consent to the

execution of a payment transaction, the payment transaction is deemed to be authorized and that the payer may authorize the payment transaction prior to its execution, or, if so agreed between the payer and his payment services provider, after the execution of the payment transaction.

From the provisions of section 10 para. 1 of the AoPS, it follows that consent to the execution of a payment transaction or of a series of payment transactions shall be granted in a form agreed upon in the contract for the provision of a single payment service or a framework contract between the payer and his payment services provider, and, if such consent is absent, the payment transaction shall be considered to be unauthorized.

From the provisions of section 10 para. 1 of the AoPS, it follows that the payment services provider is required to prove that the payment transaction was authenticated, duly recorded, accounted for and that it was not affected by any technical malfunction or other defect, in the event the payment services user denies having executed the payment transaction or claims that the payment transaction was executed incorrectly.

From the provisions of section 10 para. 2 of AoPS, it follows that if a payment services user denies having authorized an executed payment transaction, and the use of a payment instrument was recorded by the payment services provider, then the sole use of a means of payment is not sufficient proof that the payer had authorized the given payment transaction or caused an unauthorized execution of the payment transaction as a result of deception, deliberate omission, grossly negligent conduct or failure to comply with one or more obligations under section 26.

From the provisions of section 11 para. 1 of the AoPS, it follows that the payment services provider shall, without undue delay, reimburse the payer the amount of an unauthorized payment transaction, unless provided for otherwise under this Act, and where possible, restore the balance of the payment account to correspond to the balance which would have existed if the unauthorized payment transaction had not taken place; this does not affect the provisions of section 9.

From the provisions of section 12 para. 1 of the AoPS, it follows that the payer bears a loss up to €100, which is related to any unauthorized payment transactions and resulting from the use of a lost or stolen payment instrument, or from the misuse of a payment instrument by an unauthorized person due to negligence of the payer regarding the safeguarding of personalized security features according to section 26 letter c), unless paras. 2 to 4 provide otherwise.

From the provisions of section 12 para. 3 of the AoPS, 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, on condition that they prove that the breach of duties was caused by circumstances excluding liability, or proceeds according to a special regulation.

From the provisions of section 26 letter b) of the AoPS, it follows that the payment services user, 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.

Based on the evidence gathered, and according to the above-cited provisions, the court concluded that the claim was brought reasonably and therefore should be granted it in its entirety. The claim that the plaintiff has not sufficiently secured his computer using a sufficient authorized program, has not been proven by the defendant. It is not possible to consider the plaintiff negligent when they provide confidential data to a person that informs him, on a holiday, that suspicious transactions are taking place on his account. A typical bank client with average computer skills may not have sufficient specialized knowledge to recognize that there is a virus that is responsible for generating a fictitious internet banking site, or to know in detail the working procedures of the bank. The plaintiff did not give consent to the execution of the payment transactions in dispute and therefore the payment transactions cannot be considered authorized. The plaintiff personally filed a complaint regarding the movements concerning the account to which he had not given consent. This was on the earliest possible date, 06.12.2010. Moreover, the defendant himself 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 plaintiff was the successful party in the proceedings, so the court, in accordance with section 142 para. 1 of the Civil Procedure Code, awarded court costs, consisting of the court fee in the amount of €209 and attorney's fees in the amount of €665.26 (four acts of legal aid at €131.13 each, flat rate 3 times €7.41 and once €7.63, 20% VAT).

Instruction:

This judgment can be appealed, at the District Court Trenčín, within 15 days of service.

The appeal shall, in addition to the general requirements (the court to which it is addressed, who submits it, the matter it concerns and its purpose, signature, date) state, against which decision it is directed, to what extent the decision is appealed, how the decision or procedure of the court is deemed to be incorrect and what the appellant seeks. Appeals must be submitted in two copies, if the appellant fails to submit the required number of copies, the court will make the necessary number of copies at the appellant's expense (section 42 para. 3, section 205 para. 1 CPC).

An appeal against a judgment or an order, by which a decision in the main proceedings was made, can be based only on the grounds that:

- a decision has been made in a matter that falls outside the jurisdiction of the courts,

- a person who appeared in the proceedings as a party had no legal capacity to be a party to the proceedings,

- a party to the proceedings had no procedural capacity and was not properly represented,

- in the same matter there has previously been a final decision or in the same matter a prior proceeding has already begun,

- no motion to initiate the proceedings was submitted, although according to the law it was required,

- the court has deprived a party of its capacity to act before the court,

- an excluded judge has decided,

- the Court of First Instance erred in law in the matter, and therefore failed to consider other proposed evidence,

- the procedure has a different defect which could result in an incorrect decision in the case

- the Court of First Instance found incomplete facts of the case, because it did not examine the proposed evidence necessary to determine the relevant facts,

- the Court of First Instance came to the wrong conclusions based on the examined evidence,

- the facts of the case found up to that point cannot stand, because there are other facts or other evidence which have not been submitted yet (evidence concerning the conditions for the proceedings, substantive jurisdiction, exclusion of a judge, evidence to demonstrate that the procedure was defective which could result in a wrong decision. In this case, the appellant was not properly instructed under section 120 para. 4, the party, through no fault of their own could not have identified evidence or submitted it before the decision of the Court of First Instance),

- the decision of the Court of First Instance is based on a faulty legal assessment of the case (section 205 para. 2, section 205 para. 1, section 221 para. 1 of the CPC).

If the defendant fails to comply with an obligation imposed by this judgment, the plaintiff may seek its fulfillment through execution of the judgment.