COMMENTARY:

Slovak case law on the responsibility of a bank for unauthorised financial transactions

By **Rowan Legal**

Summary of the judgment of the Trenčín District Court no. ref. no: 21C/143/2011 as confirmed by the judgment of the County Court Trenčín ref. no: 17Co/213/2012 on 19 June 2013

The plaintiff: U. A. I., a citizen of the Slovak Republic against the defendant: Všeobecná úverová banka, a.s.

The plaintiff requested that the defendant bank pay €3,485.60 which had been deducted from their current account without their authorisation. The investigation by the bank found that the computer which the plaintiff had been using to log on to the internet banking site was infected by a computer virus. Once the computer was infected, the virus activated and generated a web page in the internet browser which attempted to emulate the design of the bank's internet banking site. The purpose of this fraudulent site was, by deception, to elicit sensitive authentication data and then send them to an unknown perpetrator. The thief, 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 them that the bank had registered an attempt to execute a suspicious transaction and that to cancel it, it was necessary to provide authentication using a position on the GRID card.[1] The plaintiff provided the authorization element – the requested position on the GRID card – which was in fact then used by the perpetrator to authorize the execution of the payment.

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. The obligations of the payer are outlined in section 12 of the Act so that the payer, under para. 1, shall bear the loss relating to any unauthorized payment transactions up to €100. Pursuant to section 12 para. 2 of the Act, the payer is to bear all the losses associated with the unauthorized payment transaction if it was caused by non-fulfilment of one or more obligations stated under section 26 of the Act, as a result of their gross negligence.

The defendant argued that the unauthorised payment transaction was caused as a result of the gross negligence of the plaintiff to comply with their obligation under section 26 of the Act, namely under letter a) – to use the payment instrument in accordance with the conditions governing the issuing and use of this payment instrument. Consequently the defendant claimed that the plaintiff should bear the losses relating to the unauthorized payment.

The defendant argued that the gross negligence was caused by the fact that the plaintiff, in connection with executing the payment transaction in question, gave their identification data to a person who introduced himself as an employee of the appellant and that the plaintiff had not sufficiently secured their computer using an authorized program. The defendant emphasized that with each login to the internet banking platform, the plaintiff had the opportunity to carefully go through the information presented, in particular with a strong emphasis that customers shall 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 access or authentication data. Such notices for

[1] A GRID card can be a physical item or in PDF format, comprising combinations of letters and numbers or both letters and numbers in rows and columns that is used as a method of ensuring that an end user is who they claim to be by requiring them to enter values from specific cells in a grid whose content should be only accessible to the customer and the bank.

customers is formulated very simply and clearly, and also includes demonstrations and examples of similar malicious attacks.

The court dismissed the defendant's arguments and stated that it is not possible to consider that the plaintiff was negligent if they provide confidential data to a person that informs them, on a holiday that suspicious transactions are taking place on their account. Moreover, a typical client of the bank with average computer skills may not have sufficient expertise 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 as authorized. Therefore, the court held that the defendant is obliged to pay the plaintiff €3,485.60 with interest of 9.25% per annum from 7 January 2011 until payment, within three days from the effective date of this judgment. The County Court, as an appellate court, subsequently upheld this judgment of the District Court.