

The 'man-in-the-middle attack', the unauthorized payment transaction, or whom does the law protect in online banking?

A 'man-in-the-middle-attack' is a kind of cyberattack that became widely known since 2017; it involves hackers intercepting an actual online exchange or data transfer between two parties, then occupying 'the place in the middle' and taking advantage of the thus accessed information, typically with criminal intent. Also in 2017 it was found out that users of mobile banking applications are the victims of this type of attack. What is worth noting in this case is that the third-party interference remains unnoticed as it leaves no trace, nothing that can be used subsequently as evidence to substantiate a claim that the attack actually occurred. Thus, in online banking transactions, the 'man-in-the-middle-attack' technique is used for replacing the IBAN of the recipient's bank with another one, without the user of the payment service ever becoming aware of the switch, whereas no electronic evidence can be found of unauthorized access to the online banking transaction. In that case, subject to legal dispute is whether the transaction was authorized by the payer or not.

The general rule underlying the Payment Services and Payment Systems Act (PSPSA) is that the bank will be held liable for any unauthorized transaction performed by it, except in cases where the client acted fraudulently or, whether deliberately or through gross negligence, failed to comply with one or more of the terms and conditions of issue and use of the relevant payment instrument.

Whenever a 'man-in-the-middle-attack' occurs in the process of online banking, although the payer using the identification tools supplied to him/her by the bank did not, in actual fact, consent to the execution of the payment transaction to the substitute IBAN, the bank records show him/her and no one else as the party performing the online banking transactions.

The general terms of service of banks, in line with the explicit provision of PSPSA with respect to users (who are not consumers) of banking services, make it incumbent upon a client who claims that he/she did not authorize the execution of a payment transaction to bear the burden of proof in establishing the authenticity of the same.

Thence two questions arise: if the IBAN has been replaced by another one as a result of a 'man-in-the-middle-attack', should the payment transaction be deemed unauthorized, and should the bank be held liable to reimburse the client for the lost funds.

In a court dispute concerning reimbursement of funds lost in such a transaction, this law firm

The 'man-in-the-middle attack', the unauthorized payment transaction, or whom does the law protect in online banking?

pleaded on behalf of our client that the adverse effects of the wrongful execution of a payment transaction, albeit ordered using a payment instrument accepted by the parties, should remain a legal concern for the payer solely if the bank is able to prove an act of fraud, criminal intent or gross negligence on the part of the user of the payment service, resulting in his/her failure to fulfil certain material obligations incumbent upon him/her in connection with the use of the payment instrument.

Regarding the shift of the burden of proof with respect to an unauthorized transaction as provided in the general terms of service, the Bulgarian court assumes that each of the sides to a court case should bear its own burden of proof of the facts from which it derives its rights; this, in fact, does not amount to exempting the bank providing the service from the obligation to prove its claim that the payment transaction has been duly authorized. Irrespective of the procedural law, the possibility provided by PSPSA to shift the burden of proof with respect to an unauthorized transaction to the payer comes as a result of the transposed Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market. It was exactly the need for proper interpretation of the relevant language in the Directive that has prompted Tribunal Judicial da Comarca do Porto — Juízo Central Cível to lodge a request for preliminary ruling to the Court of Justice of the European Union, in respect of which Case C-448/21 was initiated. The ruling of the Court will be of crucial importance for the implementation by the national courts of the agreement between the user (who is not a consumer) and the payment services provider in imposing more stringent liability on the payer in cases of unauthorized transactions executed via online banking, including in cases of a 'man-in-the-middle-attack'.