CASE NOTE: GERMANY

Case citation:
XI ZR 91/14

Name and level of the court:
Bundesgerichtshof (Federal Supreme Court of Germany)

Date of decision:
26 January 2016

Members of the court:
Ellenberger, Derstadt, Maihold, Dauber, Menges

Germany; evidentiary principles regarding disputed payment orders in online banking

The following summary is limited to the parts of the decision regarding the digital evidence and does not provide a full translation of the whole decision.

Facts of the case

The Respondent was a customer of and kept a business account with the Appellant. The account was usable through online banking from March 2011, allowing the managing director of the Respondent to obtain access to it by use of a personal identification number (PIN) only known to him. Transactions from the account additionally required a transaction number (TAN), for which the parties agreed on the use of an 'smsTAN-procedure', where the TAN is sent in a text message to the previously agreed telephone number. The mobile telephone containing the sim card with the respective telephone number was regularly kept by the managing director himself.

In July 2011, the Appellant modified its IT systems. During these updates, the system suffered long-lasting malfunctions, such as inaccessibility of some accounts through online banking, the failure to execute some transactions, and the double execution of other transfers. On July 15, the Respondent mistakenly received two transfers with a total of around EUR 239,000 to their account. The Appellant initiated a reversal of the transactions on July 15 and July 17, respectively, which were, due to a weekend, only processed on July 18. On July 15, the PIN of the managing director was used to query the account balance and turnover. Shortly after, a transfer of EUR 235,000 to the account of a third person was initiated, with the name of the managing director entered as 'payment details'. The Appellant sent the TAN for the transfer to the designated telephone number and it was used for authorization of the transfer. The transfer was executed on the morning of July 18, at the same time as the reversals initiated by the Appellant. As a result, the Respondent's account was left with a deficit. The Appellant unsuccessfully demanded the Respondent to balance out the deficit, and, after the Respondent's refusal, terminated the contract and filed a claim against the Respondent in the amount of the negative closing balance.

The Appellant argued that there were no irregularities recorded regarding the authorization of the transfer. The technical part was duly documented, and the Respondent did not give sufficient reason how the process may have been misused.

The Respondent argued that the managing director could not have authorized the transfer because he was on vacation at that time and had left the telephone with another employee. This employee, according to the Respondent, also did not authorize the transfer but regarded the text message as spam and deleted it.

A third party, also party in the proceedings as intervener for the Appellant, claimed to have a written order by the managing director to forward the money received on one of his accounts to another designated account. Besides that, he refused to provide more information based on his duty of confidentiality as a lawyer.

The lower courts, Landgericht Lübeck (regional court)[1] and Schleswig-Holsteinisches Oberlandesgericht in Schleswig (court of appeals)[2], both decided in favour of the Appellant.

[1] LG Lübeck, decision of 07 June 2013, file no. 3 O 418/12.
[2] OLG Schleswig, decision of 22 January 2014, file no. 5 U 87/13.

Relevant norms

While the Federal Supreme Court of Germany ('BGH') decision refers to several norms, the relevant one for the purpose of this summary is fully translated below:

§ 675w BGB

If the authorization of a processed payment transaction is in dispute, the payment service provider must prove that authentication has taken place and the payment process was duly recorded, booked and not affected by a malfunction. Authentication has taken place, when the payment service provider has verified the use of a specific payment instrument, including its personal security features, via a procedure. If the payment process was initiated by means of a payment instrument, the recording of the use of such payment instrument, including the authentication by the payment service provider as well as, if applicable, by the payment trigger service provider, is by itself not sufficient to prove that the payer

1. authorised the payment process,
2. acted fraudulently,
3. violated one or more obligations according to § 675l para. 1 BGB or
4. intentionally or grossly negligently violated one or more conditions for the issue and use of that payment instrument.

The payment service provider has to provide additional evidence to prove fraud, intent or gross negligence by the payment service user.

Summary of the decision

The BGH set aside the decision of the OLG Schleswig, returning the case to the court for further collection of evidence and final decision, taking into consideration the remarks of the BGH.

First, the BGH noted that it is undisputed that the Appellant proved the authentication of the transfer in question as well as its proper registration, documentation and trouble-free operation as required by § 675w sentence 2 BGB. As proof, the Appellant had provided a transaction protocol. According to § 675w sentence 3 no. 1 BGB, this does not necessarily prove that the transaction was authorized by the payer, though the BGH agreed with the OLG and the majority opinion that § 675w sentence 3 BGB does not exclude the use of prima facie evidence. However, the BGH decided that such prima facie evidence under § 675w BGB must meet specific criteria: the bank (in this case the Appellant) has to prove that it has a security system, which is (i) in general practically invincible and (ii) was in the individual case properly used and working faultlessly.[3] The BGH further clarified that the authentication procedure in online banking is, at the moment, regarded as invincible, if (i) it is not influenced by whether the used devices are compromised, (ii) access to the transmission route by unauthorized parties is ruled out, (iii) the (dynamic) TAN is tied to the specific transaction and (iv) the process allows the user to verify the complete and unaltered transaction before its clearance. The burden of proof regarding the invincibility lies with the bank. Unless these requirements are examined and met, the BGH found that the protocol documenting the use of PIN and the corresponding smsTAN is not sufficient to assume as prima facie evidence that it was indeed the authorized person executing the transfer. The BGH also pointed out that previous court decisions and literature did not provide assistance to determine the invincibility of a system, since these systems themselves as well as attacks on them are subject to short-term changes.[4] Therefore, the invincibility must be examined for each individual case. However, the BGH also noted that weaknesses that were discovered or became usable only after the incident in question do not stand against establishment of prima facie evidence.

Regarding the other party, here the Respondent, contesting the prima facie evidence, the BGH pointed out that he need not prove a specific and successful attack against the authentication procedure. Instead, it is sufficient to show circumstances speaking against his own involvement and suggesting the misuse by a third party. In other words: it is not necessary to prove (technical) faults of the security system, as long as he can demonstrate facts suggesting the serious possibility of a misuse. According to the BGH, this also includes circumstantial evidence outside the bank's

[3] For a similar case where the Supreme Court of Lithuania set out detailed criteria for proof, see Ž.Š. v AB Lietuva taupomasis bankas, Civil Case No. 3K-3-390/2002, Civil Chamber of the Supreme Court of Lithuania, 5 *Digital Evidence and Electronic Signature Law Review* (2008) 143 – 145 and Ž.Š. v Lietuvos taupomasis bankas, Civil case No. 3K-3-390/2002, Supreme Court of Lithuania, 6 *Digital Evidence and Electronic Signature Law Review* (2009) 255 – 262.

[4] See the discussion of this issue in the banking context in Stephen Mason and Timothy S. Reiniger, '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?', *Computer and Telecommunications Law Review*, 2015, Volume 21, Issue 5, 135 – 148.

Florian Büth is a recent graduate of the IT Law Programme taught at the University of Tartu, Estonia.

florian.bueth@gmail.com

sphere, if the party can make substantiated claims in this regard and, if denied by the other party, prove them.[5] The claims by the Respondent that the managing director did not know the receiver of the payment was on vacation at that time and that the employee holding the telephone did not use the TAN because he mistook it for spam would have, in the opinion of the BGH, constituted such substantiated claims. However, these issues had not been examined by the lower courts. The outcome therefore depended on such examination and whether it convinces the court or not. On the other hand, the BGH did not find it necessary for the Respondent to prove e.g. a malware infection of the telephone or the accessibility of the telephone by unauthorized third parties.

Since these requirements were not examined by the OLG Schleswig, the BGH referred the case back to the OLG for further examination and decision based on these requirements.

Lastly, the BGH also examined whether the Respondent can still be held accountable for the transfer under the principles of 'authority by appearance' (*Anscheinsvollmacht*) but denied it since neither the requirements were fulfilled, nor would the principles be applicable in the first place. The BGH noted further that the requirements for claiming damages were also not fulfilled.

Final decision by OLG Schleswig

The OLG Schleswig concluded the court proceedings in this case in 2017,[6] taking into consideration the requirements stipulated by the BGH. While the court ruled in favour of the Respondent and the decision itself includes more details about the arguments from both sides, the main question of invincibility of the Appellant's system remained unanswered. The reason for this was that the system, according to the Appellant, had since the incident been updated to a point where it was not possible to reconstruct the exact status it was in while the incident in question took place, thus making it impossible to be examined.

[5] This can be difficult. In the context of England and Wales and the presumption that computers are reliable, see on this point Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), 6.193 – 6.196.

[6] OLG Schleswig, decision of 09 March 2017, file no. 5 U 87/13.