Still no final clarification on victim's liability in banking phishing attacks

August 19 2016 | Contributed by Graf & Pitkowitz

Introduction
Facts
Supreme Court decision
Comment

AUTHOR

Stephan Schmalzl

Introduction

In a recent decision(1) the Supreme Court dismissed a victim's claim to refund the amount of an unauthorised payment transaction against his bank and held that:

- a payer will be considered to have acted negligently if he or she enters multiple indexed transaction numbers (iTANs) in a malicious website resembling the design of the bank's online banking platform, despite having received prior warnings by the bank;
- the maximum liability under the Federal Payment Services Act(2) for slight negligence can be waived between banks and micro-enterprises; and
- a bank (in its capacity as a payment services provider under the Federal Payment Services Act) may offset its obligation to refund an unauthorised payment transaction with its claim for damages against the accoun tholder.

Facts

The two plaintiffs ran a bed and breakfast and their joint bank account was opened as a business account. They used the account and their bank's online banking portal for private and commercial purposes. In May 2011 the plaintiffs' computer was infected with a computer virus (Spyeyes Trojan). Although the first plaintiff denied disclosing unused iTANs by entering the numbers into a forged website, the first-instance court held that, based on the number of unauthorised payment transactions, the scammer had access to all or the majority of the first plaintiff's unused iTANs. Further, the court held that there was no alternative to the iTANs having been disclosed by the first plaintiff during the phishing attack. The first plaintiff also failed to inform the bank of any unusual circumstances when using the online platform or entering the iTANs, as well as to request that the account be blocked. By using the plaintiff's iTANs, the scammer completed four transfers totalling €42,000.

The plaintiffs requested a refund for the unauthorised payment transactions based on the respective liability of the payment service provider pursuant to Section 44(1) of the Federal Payment Services Act (implementing Article 60 of the EU Payment Services Directive (2007/64/EC)(3)). The bank denied the refund by referring to the plaintiff's gross negligence – in particular, considering:

- the frequent warnings regarding the risk of online banking on the bank's website and when providing the iTANs to the plaintiff;
- specific warnings regarding phishing attacks; and
- the bank's general terms and conditions, which included special terms for online banking.

The first-instance court and the appellate court dismissed the plaintiffs' claims.

Supreme Court decision

The Supreme Court confirmed the decisions of the lower-instance courts based on a straightforward legal assessment. However, due to the merits of the case, the court did not provide long-awaited guidance on the criteria to be applied when assessing the various degrees of fault potentially limiting the liability of payment service users pursuant to Section 44(2) of the Federal Payment Services Act (implementing Article 61 of the Payment Services Directive).

In short, the Supreme Court confirmed that, in accordance with the prevailing opinion of legal scholars and German jurisprudence,(4) a payment service provider may lawfully offset claims for damages arising from the negligent behaviour of a payment service user against a user's claim to refund unauthorised payment transaction services.

As regards the question of whether the maximum liability amount for slight negligence pursuant to Section 44(2) of the Federal Payment Services Act can validly be waived between payment service providers and micro-enterprises, the Supreme Court held that when implementing the Payment Services Directive, the Austrian legislature voluntarily chose not to make use of the possibility to treat micro-enterprises in the same way as consumers. Accordingly, payment service providers may validly use framework contracts containing provisions that deviate from Sections 44(2) and (3) of the Federal Payment Services Act and micro-enterprises cannot defend themselves by alleging that these provisions are grossly disadvantageous (Section 879(3) of the General Civil Code). The Supreme Court also strengthened this assessment by referring to the fact that Austrian tort law does not provide for a limitation of liability in case of slight negligence.

Finally, the Supreme Court held that the plaintiffs had opened the bank account in relation to their business activities, rather than in their capacity as consumers. The subsequent use of a bank account for private activities does not retroactively change its qualification as a business-related account at the relevant point in time (ie, when the bank account was opened). Based on these findings, the Supreme Court held that the provision waiving the limitation of liability for slight negligence pursuant to Section 44(2) of the Federal Payment Services Act was validly agreed between the plaintiffs and the bank.

Considering that the waiver of the limitation of liability was valid, the Supreme Court limited its assessment of the first plaintiff's behaviour when entering the iTANs to the question of whether he had acted negligently. The Supreme Court confirmed slight negligence by referring to the fact that the plaintiff:

- used the online banking portal for several years and should have been aware of the fact that only one iTAN was needed to instruct a transfer; and
- ignored warnings issued by the bank regarding the risks of phishing attacks and complied with the – highly unusual – request to enter several or all iTANs in the course of the online payment procedure without becoming suspicious and informing the bank.

Comment

The Supreme Court's decision is the first to address a victim's liability for damages after a phishing attack. Due to the facts of this case, the Supreme Court limited its assessment to the question of whether the plaintiff had acted negligently. However, one section of the court's decision may provide some additional guidance. By using careful wording, the Supreme Court stated that when assessing the standard of due care, it may be necessary to consider how the iTANs were provided (eg, were they given over the phone, in an email (possibly one with poorly drafted language) or on a forged website which resembles the payment service provider's website).

Even with the Supreme Court's view regarding the scenario in which the phishing attack occurred, the court applied a user-friendly assessment when considering the facts at hand. In particular, the fact that the plaintiff entered the majority or all of the previously unused iTANs – despite never being asked for more than one iTAN before – could have been seen as gross negligence, regardless of whether the governing terms of use explicitly stated that only one iTAN would be used to confirm transactions on the online banking platform. This interpretation would be in line with German jurisprudence,(5) which provides that negligence is not based on the payer becoming a victim of a

phishing attack, but rather on the fact that the payer failed to recognise an attack, despite concrete indications and by ignoring warnings.

From a procedural standpoint, the statutory distribution of the burden of proof and, in particular, the requirements regarding *prima facie* evidence that the transaction was not sufficiently authorised (Section 34 of the Federal Payment Services Act, implementing Article 59 of the Payment Services Directive), must be carefully tailored to the changing quality of internet payment frauds – in particular, phishing attacks are becoming increasingly sophisticated, as is the use of social engineering.

This becomes an even more pressing concern considering:

- the looming transposition of the EU Revised Payment Services Directive (2015/2366/EU);
- the introduction of new third-party payment providers (offering payment initiation services/account information services);
- technical issues regarding the timely implementation of the technical standards to ensure two-factor authentication; and
- the additional risk of attacks against common two-factor authentication measures (eg, phishing or man-in-the-middle attacks against one-time passwords).

One of the cornerstones of the Revised Payment Services Directive – strong customer authentication practices – is impeded by the fact that the legislature must keep pace with technological developments in the rapidly evolving financial and IT industry. Existing best practices will most likely be outdated once the Revised Payment Services Directive comes into force and may, in the meanwhile, negatively impact the development of the digital single market. In any case, authentication must be constantly aligned with new technical developments. Further, internet payment service users must adapt to these new requirements and the potentially amended scope of diligence to ensure that they recognise attacks by correctly understanding warning signs and adhering to warnings provided by their payment service providers.

For further information on this topic please contact Stephan Schmalzl at Graf & Pitkowitz by telephone (+43 1 401 17 0) or email (schmalzl@gpp.at). The Graf & Pitkowitz website can be accessed at www.gpp.at.

Endnotes

(1) OGH 15.03.2016, 10 Ob 102/15w.

(2) Federal Payment Services Act, BGBl I 66/2009, as amended.

(3) EU Directive 2007/64/EC of the European Parliament and the Council of November 13 2007 on payment services in the internal market.

(4) BGH 24.04.2012, XI ZR 96/11, OLG Munich 23.01.2012, 17 U 3527/11.

(5) BGH 24.04.2012, XI ZR 96/11 RN 36.

The materials contained on this website are for general information purposes only and are subject to the disclaimer.