PROTECTION OF A BANK´S CLIENTS AGAINST PAYMENT FRAUDS BASED ON SOCIAL ENGINEERING: WHAT WILL UPCOMING PAYMENT SERVICES REGULATION CHANGE?

"Internationales Rechtsinformatik Symposion 2024"

Anežka Karpjáková

Keywords: ***Payment fraud, social engineering, liability for unauthorized transactions, anti-fraud measure***

Abstract: *In recent years, the number of fraudulent payment transactions in Europe has significantly increased, when fraudsters use social engineering methods (e.g. phishing or vishing) to manipulate a victim into sharing sensitive personal data or making payment transactions in favor of a fraudster. Concerning the fact that these types of fraud have become more sophisticated, it is still very difficult for potential victims to detect fraudulent behavior. Current anti-fraud measures in PSD2 seem to be insufficient in relation to these new types of fraudulent practices. Due to this fact, the European Commission recently published a proposal for the Regulation of payment services in the internal market, which updated the rules of payment services and strengthened measures to combat payment fraud. The paper introduces the EU proposal in the context of the protection of bank clients against payment fraud based on social engineering methods. The author will mainly focus on the comparison of proposed measures with the current legal framework and its evaluation.*

1. Introduction

The payment services market has changed significantly due to digitalization in recent years. Electronic payments have been constantly growing, which brings plenty of benefits to both payment institutions and clients, but also greatly increases cyber risks in this area. Currently, the banking and financial sector has been one of the areas most affected by cyber threats in the European Union (hereafter referred to as "EU").[1] Cyber attacks can target not only financial institutions, but also their clients, who are increasingly becoming victims of payment fraud.

In recent years, the number of cyber attacks against bank clients has substantially increased among EU member states, especially those based on social engineering methods.[2,3] In these cases, attackers use various forms

[1] According to the study by the European Union Agency for Cybersecurity (ENISA) in 2022 9 % of all cybersecurity threads occurred in the banking and financial sector. In: Cybersecurity: main and emerging threats. [online]. *europarl.europe.eu*, 21.3.2023. [Accessed 29. 10. 2023]. https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats.

[2] Ironically, due to advancements in cybersecurity measures in the banking and financial sector, attackers have started to use humans to acquire funds and information. Several studies state that nowadays approximately 80% of breaches involve the human element, whether it is for example the use of stolen credentials, phishing or misuse. In: E.g. DBIR Data Breach Investigations Report 2022 [online]. *verizon.com*, 2022, p. 33 [Accessed 29. 10. 2023].

[3] The term „social engineering" refers to a wide range of practices that aim to exploit human error or human behavior with the objective of gaining access to information or services. In: ENISA threat landscape 2023: July 2022 to June 2023. [online]. *enisa.europe.eu*, 19.10.2023, p. 70 [Accessed 29. 10. 2023]. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

of manipulation to trick potential victims into making mistakes, sharing sensitive payment data[4] (e.g. user ID and password for internet banking, bank account number, PIN code, or payment verification code) or transferring money from the victim´s account directly to the account controlled by the attacker.[5] Attackers also use different methods to contact potential victims, such as phishing (through email or social networks)[6], vishing (via phone call), or smishing (through SMS).[7]

Nowadays, attackers often prefer using social engineering methods over more technology-oriented attacks (e.g. using DDoS, malicious program or botnets[8]), because they are less expensive, relatively effective and more difficult to attribute to an offender.[9] Furthermore, present social engineering attacks have become more sophisticated, so for potential victims, detecting fraudulent activities can be considerably difficult. These successful frauds often result in significant financial losses for the bank‘s client, but can also lead to reputational risk for the payment institution or affect trust in the financial system.

The current EU regulation of payment services (particularly Directive (EU) 2015/2366 on payment services in the internal market (hereafter referred to as “PSD2”)[10] stipulates several measures to reduce the risk of payment fraud and increase consumer protection against them. However, these measures seem insufficient to prevent from these types of fraud, which bets on convincing the bank‘s clients to perform a certain action by themselves.[11] Regarding this fact, the European Commission (EC) in June 2023 published two legislative proposals, which are purported to update rules on payment services and strengthen measures to combat payment fraud (more below).[12]

This paper aims to introduce the crucial anti-fraud measures stipulated in these EU proposals in the context of the protection of bank clients against payment frauds based on social engineering. The author will mainly focus on the comparison of certain proposed measures with the current legal framework (PSD2) and its evaluation.

2. Anti-fraud measures in the light of current EU regulation

As mentioned above, the EU´s directive PSD2 stipulates several measures to prevent payment fraud risks and enhance the protection of customers against them. Within implementation of PSD2 had a significant impact on reducing payment frauds, particularly the introduction of a requirement for payment service providers

4 Thereafter, the stolen data are most often used to gain access to Internet banking and make fraudulent payment transactions. However, in some cases, the attacker sells the stolen data to another person (for example via the darknet) In: HOWELL, Christian Jordan. New research shows that darknet markets net millions selling stolen personal data. [online]. *fastcompany.com*, 17.7.2022. [Accessed 29. 10. 2023]. https://www.fastcompany.com/90819283/new-research-shows-that-darknet-markets-net-millions-selling-stolen-personal-data.

5 2022 Payment Threats and Fraud Trends Report. [online]. *European Payments Council*. 23.11.2022, p. 55 [Accessed 29. 10. 2023]. European Payments Council, https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-12/EPC183-22%20v1.0%202022%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf.

6 Nowadays attackers often use the method so-called „spear phishing“, which is very similar to phishing but highly targeted and individual. Attackers personalize communications based on specific information about the victim to appear even more convincing. In: Cybersecurity: social engineering. [online]. *consilium.europe.eu*, 16.10.2023. [Accessed 29. 10. 2023]. https://www.consilium.europa.eu/en/policies/cybersecurity/cybersecurity-social-engineering/.

7 Ibidem.

8 Milik, Piotr, Pilarski, Grzegorz. Cyberattacks and the bank’s liability for unauthorized payment transactions in the online banking system – theory and practice. *Cybersecurity and Law*, 2023, vol. 9, no. 1, p. 112.

9 ENISA threat landscape 2023: July 2022 to June 2023. [online], p. 71.

10 Full title: Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

11 Commission staff working document impact assessment report Accompanying the documents Proposal for a regulation of the European Parliament and the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 and Proposal for a Directive of the European Parliament and the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, p. 18.

12 Modernising payment services and opening financial services data: new opportunities for consumers and businesses. [online]. *ec.europe.eu*, 28.6.2023. [Accessed 10. 12. 2023]. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543.

(hereafter referred to as "PSP")[13] to ensure *strong customer authentication* (SCA) and an establishment of a liability framework for unauthorized payment transactions. Due to this fact, this paper will focus more deeply on these two institutes in the following subchapters.

2.1. Strong customer authentication

The PSD2 stipulates that for the initiation and processing of electronic payments by clients (payers), PSP must authorize their access using strong customer authentication. *Strong customer authentication* (SCA) involves at least a two-phase authentication of a payer's identity.[14] Client authentication is considered to be strong if it is based on two or more unique elements a client possesses in the process of authenticating a payment such as knowledge (e.g. PIN or password), possession (e.g. phone or another device) and inherence (e.g. fingerprint, voice recognition). These elements must be independent of each other, so the breach of one element does not compromise the reliability of the others.[15]

Although SCA has shown itself to be highly effective in reducing payment fraud,[16] not all types of fraudulent activities can be easily tackled by SCA. For instance in the case of an *Authorised Push Payment fraud* (APP),[17] when the fraudster convinces the bank´s client to transfer money directly to the account controlled by the attacker. Unfortunately, in these situation SCA is ineffective.[18]

2.2. Liability for unauthorized payment transaction

Directive PSD2 also deals with the question of *liability for financial losses caused by an unauthorized payment transaction* (i.e. payment transactions with the absence of payer´s consent).[19] In the author´s opinion, this regulatory framework can be considered crucial in the relation of payment frauds based on social engineering methods, because most often the fraudster carries out the payment transaction himself based on the data obtained from the bank client. These transactions are legally qualified as unauthorized.

According to the fact that in most cases of online financial fraud the identity of the attacker remains unknown and it is often impossible to claim damages from the fraudster, the PSD2 allocates liability between the payer´s PSP and the payer (bank client).[20][21] Article 73 PSD2 stipulates that liability for unauthorized payment transactions should lie primarily with the payer´s PSP.[22] Nevertheless, PSD2 stipulates several exceptions to this rule. In the context of this paper, the most relevant one is stipulated in Article 74 para. 1 PSD2, which states that the payer shall bear all of the losses relating to any unauthorized payment transactions if he fails to

[13] The term "payment service provider" (PSP) includes not only banks (credit institutions), but also non-bank entities providing payment services, e.g. electronic money institutions, payment institutions or the ECB and national central banks when not acting in their capacity as a monetary authority or other public authorities (the exhaustive list of subjects matter is contained in Article 1 (1) PSP2).

[14] Article 97 of PSD2.

[15] Article 4 para. 30 of PSD2.

[16] Commission staff working document impact assessment report Accompanying the documents Proposal for a regulation of the European Parliament and the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 and Proposal for a Directive of the European Parliament and the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, p. 8.

[17] APP fraud occurs when a client is tricked into authorizing a payment transaction to a different account, which he believes is of a legitimate payee, but this account is controlled by a fraudster. In TAYLOR, John L., GALICA, Tony. A New Code to Protect Victims in the UK from Authorised Push Payments. *Banking & Finance Law Review,* Toronto, 2020, vol. 35, no. 2, p. 327.

[18] Ibidem, p. 9.

[19] Article 64 of PSD2.

[20] Article 73 and 74 of PSD2.

[21] PSD2 defines the term „payer" as „*a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order*." In: Article 4 para. 10 of PSD2.

[22] In these cases, the payer's PSP should refund the payer the amount of the unauthorized payment transaction immediately (no later than by the end of the following business day). In: Article 73 para. 1 of PSD2.

fulfill one or more of the obligations set out in Article 69 with *gross negligence*. Article 69 of PSD2 includes an obligation for clients to use the payment instrument (e.g. credit card or internet banking) in accordance with the contract terms. In addition, this provision stipulates the duty to notify to PSP without undue delay on becoming aware of the loss, theft, misappropriation or unauthorized use of the payment instrument.

It is important to note that the concept of gross negligence is not defined in PSD2. The directive allows member states to determine the institute of gross negligence in their national law.[23][24] However, the wording of the national rules in many EU member states gives no further guidance on how to interpret the concept of gross negligence in this context, including for example Czechia, Denmark, Norway, Sweden etc.[25] Also due to this fact, courts in different Member States have adopted different approaches to what should be considered the grossly negligent behaviour.[26]

Unfortunately, in the vast majority of cases among EU member states, the PSPs refuse the payer´s claim for reimbursement with the argument that the payer has acted with gross negligence when the payer e.g. voluntarily shared sensitive information with the fraudster. Until now, the glaring exception is Netherlands, where, in 2022, 89% of cases saw customers reimbursed voluntarily within the leniency program of four major Dutch banks.[27]

3. Measures according to upcoming regulation

On 28 June 2023, the European Commission (EC) published the *Payment Services package*, which should completely replace the current directive PSD2. The package includes two legislative proposals, namely i) a revised Payment Services Directive (also known as "PSD3 proposal")[28] and ii) Payment Services Regulation in the internal market (hereafter referred to as "PSR proposal").[29][30] However, in the context of this paper, only the PSR proposal is particularly relevant, while contains several provisions that are supposed to effectively combat payment fraud and improve customer protection,[31] for example adding a confirmation of payee,[32] strengthening transaction monitoring[33] or enabling PSPs to share fraud-related information between them.[34] However, according to the limited scope of this paper, in the following subchapters, the author introduces and assesses in more detail only two of the proposed measures related to the mitigation of payment frauds, namely expansion of liability framework for unauthorized and authorized payment transactions and education awareness.

---

23 Recital 72 of PSD2.

24 However, Recital 72 of PSD 2 states that although the concept of negligence implies a breach of a duty of care, gross negligence must be more significant than mere negligence, involving conduct exhibiting substantial carelessness.

25 Kjørven, Marte Eidsand. Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe, (2020), 31, *European Business Law Review*, 2020, vol. 31, no. 1, p. 95.

26 Donelly, Mary. Payments in the digital market: Evaluating the contribution of Payment Services Directive II. *Computer Law & Security Review*, 2016, vol. 32, no. 6, p. 834.

27 Commission staff working document impact assessment report Accompanying the documents Proposal for a regulation of the European Parliament and the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 and Proposal for a Directive of the European Parliament and the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, p. 9.

28 Full title: Proposal for a Directive of the European Parliament and the Council on Payment Services and Electronic Money Services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC.

29 Full title: Proposal for a Regulation of the European Parliament and the Council on Payment Services in the Internal Market and amending Regulation (EU) No 1093/2010 (PSR proposal).

30 Financial data access and payments package. [online]. *finance.ec.europe.eu*, 28. 6. 2023. [Accessed 29. 10. 2023]. https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en.

31 Recital 3 of PSR proposal.

32 Proposal PSR requires the payee's PSPs to verify the consistency between the name and unique identifier of a payee (IBAN/name match) before the initiation of credit transfers. In: Article 50 of PSR proposal.

33 Article 83 of PSR proposal.

34 Article 83 of PSR proposal.

3.1. Liability for unauthorized and authorized payment transactions

The PSR proposal introduces a new liability framework for financial losses arising from fraudulent transactions. In comparison with the PSD2, the regulation of the liability of PSPs for unauthorized payment transactions remains virtually unchanged.[35] The PSR should newly also harmonize liability rules for authorized payment transactions. Nevertheless, according to the proposal the liability for authorized payment transactions is supposed to be limited only to very specific types of spoofing fraud.[36] The provision should only apply to situations, when the fraudster contacts the client, who is consumer,[37] pretending to be an employee of the consumer‘s PSP (unlawfully using the name, e-mail address or phone number of the consumer´s PSP) and therefore tricks the client into making a fraudulent payment transaction.[38] According to this provision, victims of “spoofing” fraud may be able to request a refund from their PSP for the full amount of the fraudulent transaction.[39] However, refunds would not be allowed in cases of client´s grossly negligent behaviour.[40] As you can see, the division of liability between PSP and its client is very similar to the legal framework for unauthorized payment transactions according to PSD2 and PSR proposal. In both cases, the PSR proposal does not clarify what criteria must be met to qualify the PSP’s client‘s actions or omissions as grossly negligent.

Based on present uncertainty about the interpretation of the term gross negligence and the unwilling attitude of PSPs to accept refunds for financial losses caused by payment fraud, the author assumes that in the overwhelming majority of cases, PSPs will continue to reject client´s requests for a refund with reasoning that client has committed gross negligence.

3.2. Education Awareness

In the author´s opinion, one of the reasons for the increasing number of successful payment frauds using social engineering methods is PSP´s client‘s inability to recognize fraudulent conduct. One of the causes may be a low level of awareness about payment fraud risks and current manipulative practices among the public.[41] Due to this fact, PSR proposal set an obligation for PSPs to carry out education actions to increase awareness of payment fraud forms and trends among their customers and staff.[42]

Nevertheless, the proposal does not specify how PSPs are supposed to alert their client about a new form of attack and how to identify them. Even though many PSPs already inform their clients about payment frauds based on social engineering in different ways, e.g. internet banking notification, warning on the official websites, it is unclear if these actions can be deemed sufficient according to PSR. From author´s point of view

35 Comparison of Article 64 of PSD2 with Article 56 and Article 60 of PSR proposal.

36 „Spoofing“ can be described as the method when fraudsters use technology to hide the actual phone number or e-mail address and display another phone number in the Caller ID or another e-mail address. In: Caller ID Spoofing. [online]. *almabank.com*. [Accessed 29. 10. 2023]. https://www.almabank.com/The-ALMA-Difference/Caller-ID-Spoofing; Attackers very often spoof the e-mail domain name or phone number of a PSP, so the potential victim can be easily tricked into sharing sensitive information in good faith that the received call/e-mail is from its bank. In: 2022 Payment Threats and Fraud Trends Report. [online]. p. 15.

37 It is important to highlight this provision is limited only to consumers. In: Recital 39 of PSR proposal.

38 Article 59 of PSR proposal.

39 Consumers must fulfill conditions stipulated in Article 59 para. 1 of PSR proposal, including filing a police report and notification to their PSP without undue delay. If the PSP accepts the request for a refund, the PSP returns a fund to the client´s bank account within 10 days.

40 Recital 82 of PSR proposal.

41 Iser, Bettina, Brandtweiner, Roman. *Role of Awareness to prevent personal disasters: reducing the risks of falling for phishing by strengthening user awareness*. p. 79–92 In: Passerini, G. et al. Disaster Management and Human Health Risk VII: Reducing Risk, Improving Outcomes, 2022.

42 Article 84 of PSR proposal.

could be one of the effective tools for example creating e-learning interactive courses, which already offers to their client for example the company Revolut Ltd.[43]

4. Conclusion

The proposed anti-fraud measures for PSR are a recognition of the changes in the fraud landscape since 2015, when PSD2 was adopted. Particularly, the PSR proposal responds to the increasing number and sophisticationž of fraud based on social engineering methods in recent years. This paper mainly focused on the liability framework for unauthorized payment transactions and for payment transactions made as a result of "spoofing" frauds. Within these provisions, the author sees certain shortcomings, particularly in the lack of clarification of the term "gross negligence". Furthermore, the paper focused on the proposal of PSP´s obligation to inform their clients about given online frauds and their new trends, because in the author´s opinion the awareness can be one of the most important factor to increase the level of protection and resilience.

Nevertheless, it is important to note that the proposal PSR is currently in the legislative stage of first reading and certain provision may still be subject to further discussions and the trilogue negotiations between the three EU institutions. According to this fact the final text of Resolution may deviate from the current proposals.

References

2022 Payment Threats and Fraud Trends Report. [online]. *European Payments Council*. 23. 11. 2022. [Accessed 29. 10. 2023]. European Payments Council, https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-12/EPC183-22%20v1.0%202022%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

Cybersecurity: main and emerging threats. [online]. *europarl.europe.eu*, 21.3.2023. [Accessed 29. 10. 2023]. https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats

Cybersecurity: social engineering. [online]. *consilium.europe.eu*, 16.10.2023. [Accessed 29. 10. 2023]. https://www.consilium.europa.eu/en/policies/cybersecurity/cybersecurity-social-engineering/

Caller ID Spoofing. [online]. *almabank.com*. [Accessed 29. 10. 2023]. https://www.almabank.com/The-ALMA-Difference/Caller-ID-Spoofing

Commission staff working document impact assessment report Accompanying the documents Proposal for a regulation of the European Parliament and the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 and Proposal for a Directive of the European Parliament and the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC. [online]. *eur-lex.europe.eu*. 28. 6. 2023. [Accessed 29. 10. 2023]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2023:231:FIN&qid=1688388693349

Donelly, Mary. Payments in the digital market: Evaluating the contribution of Payment Services Directive II. *In Computer Law & Security Review,, Vol. 32, No. 6, 827–839, 2016.*

Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2).

DBIR Data Breach Investigations Report 2022 [online]. *verizon.com*, 2022. [Accessed 29. 10. 2023]. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

ENISA threat landscape 2023: July 2022 to June 2023. [online]. *enisa.europe.eu*, 19.10.2023. [Accessed 29. 10. 2023]. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[43] E.g.: MACSIM, Miruna. Revolut launches in-app educational course to empower customers to combat fraud. [online]. *business-review.eu*. 13.9.2023. [Accessed 29. 10. 2023]. https://business-review.eu/money/banking/revolut-launches-in-app-educational-course-to-empower-customers-to-combat-fraud-251562.

Iser, Bettina. Brandtweiner, Roman. *Role of Awareness to prevent personal disasters: reducing the risks of falling for phishing by strengthening user awareness*. p. 79–92 In: Passerini, G. Et al. Disaster Management and Human Health Risk VII: Reducing Risk, Improving Outcomes, 2022.

Financial data access and payments package. [online]. *finance.ec.europe.eu*, 28.6.2023. [Accessed 29. 10. 2023]. https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en

Howell, Christian Jordan. New research shows that darknet markets net millions selling stolen personal data. [online]. *fastcompany.com*, 17.7.2022. [Accessed 29. 10. 2023]. https://www.fastcompany.com/90819283/new-research-shows-that-darknet-markets-net-millions-selling-stolen-personal-data

Kjørven, Marte Eidsand. Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe, (2020), 31, *European Business Law Review*, 2020, vol. 31, no. 1, pp. 77–109.

Modernising payment services and opening financial services data: new opportunities for consumers and businesses. [online]. *ec.europe.eu*, 28.6.2023. [Accessed 10. 12. 2023]. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543

Milik, Piotr, Pilarski, Grzegorz. Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system – theory and practice. *Cybersecurity and Law*, 2023, vol. 9, no. 1, pp. 108–126.

Macsim, Miruna. Revolut launches in-app educational course to empower customers to combat fraud. [online]. *business-review.eu*. 13. 9. 2023. [Accessed 29. 10. 2023]. https://business-review.eu/money/banking/revolut-launches-in-app-educational-course-to-empower-customers-to-combat-fraud-251562

Taylor, John L., Galica, Tony. A New Code to Protect Victims in the UK from Authorised Push Payments. *Banking & Finance Law Review,* Toronto, 2020, vol. 35, no. 2, pp. 327–332.

Proposal for a Regulation of the European Parliament and the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 (PSR proposal).

Proposal for a Directive of the European Parliament and the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC (PSD3 proposal).

Payment services: revised rules to improve consumer protection and competition in electronic payments. [online]. *ec.europe.eu*, 28.6.2023. [Accessed 29. 10. 2023]. https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3544