Authorized Push Payment Fraud: Suggestions for the Draft Payment Services Regulation

Authorised Push Payment Fraud: Suggestions for the Draft Payment Services Regulation

Abstract English

This article addresses the rising prevalence of Authorised Push Payment (APP) fraud in the digital payment landscape and the need for new regulations by the EU legislature. APP fraud, where the payment service user (PSU) authorizes a payment under the influence of a fraudster, presents a growing issue that is inconsistently addressed under the current EU Payment Services Directive (PSD2). The article analyzes existing legal frameworks and case law across various EU member states, highlighting inconsistencies in the interpretation of authorised and unauthorised transactions. It emphasizes the need for the EU legislature to clarify liability for payment service providers (PSPs) in the proposed Payment Services Regulation (PSR) regarding APP fraud. The authors advocate for a harmonized approach where PSPs are held liable for APP fraud, particularly in cases of bank impersonation fraud. The authors further suggest that the definition of "gross negligence" in the context of APP fraud should be clarified. They also propose that if PSPs take on greater responsibility for fraud monitoring and prevention in order to improve safety of payment transactions this should be balanced with the privacy and autonomy of the PSU. Key conclusions include the necessity for the EU legislature to ensure a uniform interpretation of authorised transactions and clarify the potential for national liability rules. Additionally, the authors recommend that liability for APP fraud should not be limited to bank impersonation fraud but should also cover other scenarios of payment fraud, provided the fraudster abuses the trust in the payment system by convincing the PSU that he needs to take action to keep his funds safe.

Zusammenfassung

Dieser Artikel behandelt die zunehmende Verbreitung von Betrug durch autorisierte Push-Zahlungen (*APP fraud*) im digitalen Zahlungsverkehr und die Notwendigkeit neuer Vorschriften durch den EU-Gesetzgeber. APP fraud, bei dem der Zahlungsdienstnutzer (PSU) eine Zahlung unter dem Einfluss eines Betrügers autorisiert, stellt ein wachsendes Problem dar, das unter der aktuellen EU-Zahlungsdienste-Richtlinie (PSD2) uneinheitlich behandelt wird. Der Artikel analysiert bestehende Rechtsrahmen und Rechtsprechung in verschiedenen EU-Mitgliedstaaten und hebt Inkonsistenzen in der Interpretation von autorisierten und nicht autorisierten Transaktionen hervor. Er betont die Notwendigkeit, dass der EU-Gesetzgeber in der vorgeschlagenen Zahlungsdienste-Verordnung (PSR) die Haftung der Zahlungsdienstleister (PSP) bei APP-Betrug klärt. Die Autoren plädieren für einen harmonisierten Ansatz, bei dem PSPs für APP-Betrug haftbar gemacht werden, insbesondere in Fällen von Bankimitationsbetrug (*bank impersonation fraud*). Die Autoren schlagen auch vor, die Definition von "grober Fahrlässigkeit" im Kontext von APP-Betrug zu klären. Sie schlagen außerdem vor, dass PSPs, wenn sie mehr Verantwortung für die Betrugsüberwachung und -prävention übernehmen, um die Sicherheit von Zahlungstransaktionen zu verbessern, dies mit der Privatsphäre und Autonomie des PSU abwägen sollen. Zu den wichtigsten Schlussfolgerungen gehört die Notwendigkeit, dass der EU-Gesetzgeber eine einheitliche Interpretation von autorisierten Transaktionen sicherstellt und den Spielraum für nationale Haftungsregeln klärt. Darüber hinaus empfehlen die Autoren, dass die Haftung für APP-Betrug

nicht auf Bankimitationsbetrug beschränkt sein sollte, sondern auch andere Szenarien von Zahlungsbetrug umfassen sollte, sofern das Vertrauen der Menschen in das Zahlungssystem vom Betrüger missbraucht wird, indem er den PSU davon überzeugt, dass er Maßnahmen ergreifen muss, um seine Gelder zu schützen.

Résumé
Cet article, aborde la prévalence croissante de la fraude par paiement push autorisé (APP) dans le paysage des paiements numériques et la nécessité de nouvelles réglementations par le législateur de l'UE. La fraude APP, où l'utilisateur du service de paiement (PSU) autorise un paiement sous l'influence d'un fraudeur, présente un problème croissant qui est traité de manière incohérente sous la directive actuelle sur les services de paiement de l'UE (PSD2). L'article analyse les cadres juridiques existants et la jurisprudence dans divers États membres de l'UE, mettant en évidence les incohérences dans l'interprétation des transactions autorisées et non autorisées. Il souligne la nécessité pour le législateur de l'UE de clarifier la responsabilité des prestataires de services de paiement (PSP) dans le règlement proposé sur les services de paiement (PSR) en ce qui concerne la fraude APP. Les auteurs plaident pour une approche harmonisée où les PSP sont tenus responsables de la fraude APP, en particulier dans les cas de fraude par imitation de banque. Les auteurs suggèrent en outre que la définition de la "négligence grave" dans le contexte de la fraude APP soit clarifiée. Ils proposent également que si les PSP assument une plus grande responsabilité en matière de surveillance et de prévention de la fraude afin d'améliorer la sécurité des transactions de paiement, cela devrait être équilibré avec la confidentialité et l'autonomie du PSU. Les principales conclusions incluent la nécessité pour le législateur de l'UE de garantir une interprétation uniforme des transactions autorisées et de clarifier la portée des règles de responsabilité nationales. De plus, les auteurs recommandent que la responsabilité pour la fraude APP ne soit pas limitée à la fraude par imitation de banque, mais couvre également d'autres scénarios de fraude de paiement, à condition que la confiance des personnes dans le système de paiement soit abusée par le fraudeur, en convainquant l'utilisateur du service de paiement qu'il doit prendre des mesures pour assurer la sécurité de ses fonds.

1. Introduction[1]

1. With the digitalisation of payment services there has been an increasing prevalence of payment fraud, as well as a change in the nature of payment fraud,[2] leading to a new regulatory dilemma to be solved by the EU legislature.[3]

Historically, payment fraud was confined to stealing someone's bank credentials, for example the bank card and corresponding code. This resulted in a so-called unauthorised (payment) transaction in which the transaction was not authorised by the payment service user (**PSU**) himself, but by the fraudster. The current EU Payment Services Directive (**PSD2**)[4] provides that the payment service provider (**PSP)** of the PSU -which is

---

1 The coordinating author of this article is E.J. van Praag (the Netherlands). Authors from the following countries in alphabetical order of countries participated in the drafting of this article: Belgium (R. Steennot), Norway (M. Eidsand Kjørven, V. Wold, L.P. Halvorsen Omland), Portugal (M.R. Guimarães), The Netherlands (K.J.O. Jansen, G.S. Breukelaar), United Kingdom (A. Fejős). All authors participated in the discussions about the entire article, but may not necessarily agree with everything written here.

These authors have written on various occasions about the liability for payment fraud and this article draws to an extent on ideas presented in these articles. See E.J. van Praag, *PSD2: naar open banking en bankieren in een ecosysteem (Preadvies voor de Vereniging voor Financieel Recht 2020) (Serie Van der Heijden Instituut nr. 169)*(Deventer: Wolters Kluwer 2020), pp 134-149, E.J. van Praag, *Fighting Payment Fraud: Some key considerations for the EU legislator*, Oxford Business Law Blog 9 September 2024, M. Eidsand Kjørven, 'Who Pays When Things go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe', 31. *EBLR (European Business Law Review)*2020(1), p 88, M.R. Guimares & R. Steennot, 'Allocation of Liability in Case of Payment Fraud: Who bears the Risk of Innovation? A Comparison of Belgian and Portuguese Law in the Context of PSD2', 30. *ERPL* (*European Review of Private Law)* 2022(1), p 29, M.R. Guimarães, 'Na minha conta ou na tua?" Revisitação do regime aplicável às operações de pagamento fraudulentas à luz da nova Proposta de um Regulamento relativo aos serviços de pagamento no mercado interno, de 28 de Junho de 2023', *A Revista*, *Supremo Tribunal de Justica* 2023(4), p59, V.Wold and P. Kalamees, 'Identity Theft in Consumer Finance: Consent, Contract and Liability – Analysing Rules on Loss Allocation in Norwegian, Estonian and EU Law', (forthcoming in *Oslo Law review*, 2025),U.Amajuoyi and A. Fejős, Mind the Consumer Protection Gap: the UK Financial Ombudsman Service, Fairness and Reasonableness, and the Law ' in P. Tereszkievicz and M. Golecki, *Protecting Financial Consumers in Europe* (Leiden: Brill, 2023).

2 See European Banking Authority and European Central Bank, 2024 Report on Payment Fraud, 1 August 2024, https://www.eba.europa.eu/sites/default/files/2024-08.

3 See from other authors about liability for fraudulent transactions D. McIlroy and R. Sethi-Smith, 'Prospects for bankers' liability for authorized push payment fraud', *JIBFL* (*Butterworth Journal of International Banking and Financial Law)* 2022, pp 172-175, M.C. Paglietti, 'Restitution and Liability in the Multilevel Regulatory Framework of Unauthorized Digital Payment Transactions', *ERPL* 2022(1), pp 155–190, M.C. Paglietti and M. Rabitti, 'A Matter of Time. Digital- Financial Consumers Vulnerability in the Retail Payments Market', 33. *EBRL* 2022 (4), p 602, M. Casper and B. Reich, 'Haftung bei einem qualifizierten Phishing mit weiteren Elementen des Social Engineering', 35. *ZBB (Zeitschrift für Bankrecht und Bankwirtschaf)* 2023(3), pp 133-157, M.R. Aagaard, 'Tredjemans svikliga förledande – Kan en godkänd betalningstransaktion vara obehörig?', *SVJT (Svensk Juristtidning)* 2024(5), p 323, S. Karstoft, 'Forbrugeres hæftelse for netbankoverførsler som følge af bedrageriske telefonopkald', *Erhvervsjuridisk Tidsskrift* 2024, pp 99-100, and J. Braithwaite, 'Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like', 10. *JFR Journal of Financial Regulation* 2024 (2), pp 1–20.

4 Dir. 2015/2366 of 25 November 2015 on payment services in the internal market, https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng.

often, but not always a bank-[5] is liable in case of unauthorised payments, unless the PSU failed to fulfil its obligations to keep the account safe with intent or gross negligence, or acted fraudulently.[6,7]

2. Nowadays, payment fraud also concerns social engineering; tricking the PSU into authorising himself the payment to another account. An example of this type of fraud is sending a WhatsApp message, pretending to be someone's child in urgent need of money or pretending to be the bank of the PSU, requesting the PSU to take action to keep his money safe (**bank impersonation fraud**). This type of fraud is referred to as authorised push payment fraud (**APP fraud**), because the PSU himself has authorised the payment transaction. In case of APP fraud, there is no provision in PSD2 allocating liability to the PSP. Only in some EU jurisdictions the PSU can obtain compensation from his PSP, if the PSU can substantiate that (i) the PSP had a duty of care based on national private law to monitor his transactions, (ii) should have noted that transactions were suspicious and (iii) failed to act.[8] This is a debate in the courts which PSUs hardly ever win.

3. The growth in APP fraud has led to a growing feeling of discomfort with legislators and regulators,[9] which came to the fore in the European Commission's (**EC**) proposal for a update of PSD2, which will be laid down in a regulation (the draft proposal for a Payment Services Regulation (**PSR**)).[10] PSR suggests to introduce various new ways of alleviating the problem of APP fraud for the potential victims.[11,12] Notably in PSR, the EC proposes that in case of bank impersonation fraud where a PSU was manipulated by a third party pretending to be an employee of the PSP using the name, e-mail address or telephone number of that PSP

---

5 There are also PSPs that do not qualify as banks (credit institutions), namely payment institutions and e-money institutions. As opposed to banks, they are not allowed to pay interest. Historically the majority of European consumers hold their day-to-day payment account with a bank.

6 This has been a political choice to ensure that consumers are willing to use the services of PSPs. See Dir. 2015/2366 recital (69).

7 Articles 73 and 74 Dir 2015/2366.

8 See for example Rechtbank Amsterdam 20 November 2024, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2024:7070 and Tribunal da Relação de Lisboa of 20 February 2024 (Rapporteur Rute Lopes), https://www.dgsi.pt/jtrl.nsf/ and *Tribunal da Relação de Évora* of 22 May 2014 (Rapporteur Mata Ribeiro), https://www.dgsi.pt/jtre.nsf/ and *Tribunal da Relação de Guimarães* of 17 December 2014 (Rapporteur Fernando Fernandes Freitas), https://www.dgsi.pt/jtrg.nsf/.

9 See for example Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 onpayment services in the internal market (PSD2), 23 June 2022, https://www.eba.europa.eu p 7 and p. 68 and Answer given by Ms McGuinness on behalf of the European Commission 4 May 2023, https://www.europarl.europa.eu/doceo/document/E-9-2023-000775-ASW_EN.html.

10 Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010, 28 June 2023, 2023/0210 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367, recitals (79) and (80).

11 The other main measures are: a. confirmation of payee services extension of International Bank Account Number verification to all credit transfers; b. improvements to the application of SCA; c. legal basis for exchange of information on fraud; d. educating and alerting PSUs about fraud risks; and e. enhanced transaction monitoring.

12 A critical evaluation of the measures taken so far can be found in European Court of Auditors, Special report Digital payments in the EU Progress towards making them safer, faster, and less expensive, despite remaining gaps, 2025 01, p 36.

unlawfully, and that manipulation gave rise to subsequent fraudulent authorised transactions, the PSP shall refund the PSU.[13] The exceptions are fraud and gross negligence by the PSU. This proposal seems based on the Dutch voluntary compensation scheme for bank impersonation fraud. In 2020, the members of the Dutch Banking Association agreed upon a voluntary compensation scheme, specifically for victims of bank impersonation fraud.[14],[15] This specific proposal of the EC was welcomed by the EU co-legislators,[16] although complemented by the latter with a suggestion to compensate the PSU in more scenarios than sole bank impersonation fraud. This has led to a vehement debate about which measures to take.[17]

4. In this paper we aim to give guidance to the EU co-legislators on how APP fraud should be regulated.[18] In order to do so, we also discuss how fraudulent payments are currently dealt with under PSD2. First, we explain the current PSD2 liability rules for fraudulent transactions (section 2). We then discuss whether PSP liability should extend beyond bank impersonation fraud (section 3), balancing safety with privacy and autonomy (section 4) and (harmonization of) gross negligence (section 5). We also discuss the possible liability of other parties in the fraud ecosystem, such as the PSP of the payee and electronic communications services providers (section 6). We conclude with our recommendations (section 7).

2. The current PSD2 liability rules for fraudulent transactions explained

5. Below we explain the liability rules under PSD2 for unauthorised transactions, and how authorised, but fraudulent transactions are currently dealt with.

2.1 Liability for unauthorised transactions

---

13 Article 59 Dir. 2015/2366

14 See Criteria for awarding compensation for loss arising from bank help desk scams ('spoofing'), Dutch Banking Association, 2 June 2021, https://www.nvb.nl/media/5661/criteria-for-awarding-compensation-for-loss-arising-from-bank-help-desk-scams-spoofing-june-2nd-2021.pdf.

15 There is already some case law dealing with the question when a PSU is grossly negligent in case of bank impersonation fraud and therefore not eligible for the voluntary compensation scheme. Dutch Institute for Financial Disputes 29 January 2025, 2025-0053, https://www.kifid.nl/wp-content/uploads/2025/01/Uitspraak-2025-0053.pdf.

16 See the position of the European Parliament of 23 April 2024, data.consilium.europa.eu/doc/document/ST-10664-2024-INIT/en/pdf and the preliminary position of the European Council of 14 June 2024, https://data.consilium.europa.eu/doc/document/ST-10487-2024-INIT/en/pdf. This article is up to date until April 2025. Further developments have not be taken into account.

17 See for example European Payments Institutions Federation Statement on the Authorization of Payment Transactions under the Payment Services Regulation statement of, July 2024, https://paymentinstitutions.euEPIF-statement-on-the-Authorization-of-Payment-Transactions-under-the-PSR.

18 We discuss the various points raised in the political debate. See Proposal for a Directive of the European Parliament and of 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 and Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 - Progress report, 16 December 2024, 2023/0209(COD), 2023/0210(COD), p. 23, https://data.consilium.europa.eu.

At the European level, PSD2 stipulates the obligations that PSPs and PSUs have towards each other. Two main principles apply as regards to liability for unauthorised transactions:

i. PSPs must be able to prove, upon request, that the PSU has authenticated the transaction with his payment instrument,[19] for example by demonstrating that the latter has used his bank card and entered the correct personal identification number (PIN) or that the signature is on the payment order.[20] This process of authenticating transactions is called strong customer authentication (**SCA**), when it requires a combination of at least two elements of something the client *has* (for example bank card), something the client *knows* (for example the PIN) and something the client *is* (for example his fingerprint).[21] By not requiring SCA, the PSP is automatically liable, unless the payer acted fraudulently.[22]

ii. However, even if SCA has been carried out (the bank card was used and the PIN was correctly entered), the payer's authorisation to the transaction may still be missing, for example, if his bank card and PIN were stolen.[23] In such cases, the PSP is liable, unless the payer acted fraudulently, or failed to fulfil the obligations to keep the account safe with intent or gross negligence.[24] Then the payer has to carry the loss himself. However, as a Member State option, Member States may reduce the liability of the payer, if the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations to keep the account safe. [25] Furthermore, PSD2 allows Member States to determine that in

---

19 For the definition of payment instrument see European Court of Justice 11 November 2020, *DenizBank AG/Verein für Kosumenteninformation* , C-287/19, https://eur-lex.europa.eu and European Court of Justice 11 July 2024, *UA/Eurobank Bulgaria AD*, C-409/22, https://eur-lex.europa.eu.

20 Article 72 Dir. 2015/2366.

21 See extensively article 4 (30) Dir. 2015/2366 and Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

22 Article 74 sub 2 Dir. 2015/2366.

23 See for example European Court of Justice 11 July 2024, https://eur-lex.europa.eu, Decision of the Appelate Body of the Dutch Institute for Financial Disputes 18 September 2023, 2023-0036, https://www.kifid.nl/wp-content/uploads/2023/09/Uitspraak-2023-0036.pdf. See on the other hand Gerechtshof Arnhem-Leeuwarden 24 December 2024, https://uitspraken.rechtspraak.nl/ECLI:NL:GHARL:2024:7950, no. 3.12, where the court considered that if consent to execute a transaction or a series of transactions has been given in the form agreed between the payer and the PSP, the PSP may rely on this.

24 Article 74 Dir. 2015/2366.

25 This option has been used be the legislators in Denmark, Sweden and Norway to provide statutory limits on PSU liability absent intent or fraud. In the Netherlands this Member State's option has been used to give courts discretion to partly allocate liability to the PSP, even if the payer acted grossly negligent. See 7:529 sub 2 Dutch Civil Code (**DCC**). In Portugal, where the user has neither acted fraudulently nor intentionally failed to fulfil his obligations, but only acted with gross negligence, his liability is reduced to the credit limit of the respective account or of the payment instrument, or to the limit of his available balance: see Article 115 (4), Portuguese Decree-Law 91/2018 of 12 November.

cases of unauthorised transactions, the first €50 of the damage is always the payer's responsibility.[26]

There is a significant amount of case law on when a PSU is grossly negligent and how the damages should be distributed.[27]

2.2 The current blurred distinction between authorised and unauthorised fraudulent transactions

6. Different rules apply to APP fraud. Before we discuss those different rules in section 2.3, we will first discuss how to distinguish between unauthorised transactions and APP fraud. The exact interpretations of what constitutes an unauthorised transaction differs amongst courts (or consumer complaints tribunals) in EU Member States.

7. Per the text of PSD2, a transaction is only authorised if the PSU has given his "consent" to it.[28] The key question therefore is whether for transactions that are authenticated by the PSU himself, "consent" nevertheless may be deemed missing. An interpretation is that a transaction is authorised, when the PSU instructed the PSP to credit a certain amount to a certain account (implying the fact that the payer was tricked is insufficient to determine that the transaction was unauthorised). Another interpretation is that a transaction is only authorised, when the PSU actually intended to pay a specific payee and for the right reason. Another possible view is that the customer must have at least understood that a payment transaction was being executed as a result of his actions.

8. To illustrate that the distinction differs between Member States, we point to the fact that in Sweden, Denmark and Norway, (whose private law systems are generally rather similar), the interpretation of "consent" has given rise to debate, and the law is applied differently across these three countries.[29] One discussion is the meaning of the term "consent" itself,

---

[26] For example, the Netherlands has not opted for this Member State's option. See *Kamerstukken II*, 34813, no. 19, https://zoek.officielebekendmakingen.nl/kst-34813-19.html.

[27] See for example Decision of the Appellate Body of the Dutch Institute for Financial Disputes 7 February 2025, 2025-0012, Hoge Raad der Nederlanden 21 May 2021, https://uitspraken.rechtspraak.nl/ECLI:NL:HR:2021:749, Rechtbank Amsterdam 23 January 2024, https://uitspraken.rechtspraak.nl/ECLI:NL:RBAMS:2024:441, Gerechtshof Arnhem-Leeuwarden 24 December 2024,https://uitspraken.rechtspraak.nl/ECLI:NL:GHARL:2024:7950; Dutch Institute for Financial Disputes 6 February 2025, 2025-0094, https://www.kifid.nl/wp-content/uploads/2025/02/Uitspraak-2025-0094-Bindend.pdf; Appelate Body of the Dutch Institute for Financial Disputes 15 June 2020, 2020-027,https://www.kifid.nl/wp-content/uploads/2023/09/Uitspraak-2023-0036.pdf , Bundesgerichtshof, judgment of 26 January 2016, XI ZR 91/14, https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document, Norwegian Supreme Court Case HR-2022-1752, https://www.domstol.no/globalassets/translated-rulings/hr-2022-1752-a.pdf, Swedish Supreme Court Case NJA 2022 s. 522,https://www.domstol.se/en/supreme-court/precedents-archive/case-t-4623-21/ *French Court de Cassation*, Chambre commerciale, financière et économique - pourvoi n°23-16.267, https://www.legifrance.gouv.fr/juri/id/JURITEXT000050442874, Finnish Supreme Court case HD:2018:71, https://korkeinoikeus.fi/en/index/ennakkopaatoksh/2018/kko201871.html. See also, in Portugal, Sentence of *Tribunal da Relação de Lisboa* of 13 July 2023 (Rapporteur Gabriela de Fátima Marques), https://www.dgsi.pt/jtrl.nsf, Sentence of *Tribunal da Relação do Porto* of 18 April 2023 (Rapporteur João Ramos Lopes), https://www.dgsi.pt/jtrp.nsf.

[28] Article 64 sub 1 Dir. 2015/2366.

[29] We note here that Norway, while not an EU Member State, is a member of the single market through the EEA agreement and is obligated to implement EU legislation in largely the same way as Member States.

namely the degree to which it requires a level of understanding in the mind of the PSU that he is in fact authorising a transaction. In Norway, the relevant ADR body has consistently held that a transaction is considered authorised only if the PSU is aware that he was initiating a transaction to a third party.[30] The reasoning behind this is, in a nutshell, that there is no reason to treat PSUs that have been tricked over the phone into providing security information to what they believe to be their PSP more favourably than for example PSUs being tricked into transferring funds to a designated "safe account".[31] In Sweden, however, the interpretation at the ADR level, and in a recent case from the Stockholm City Court, is more "objective", though allowances are seemingly made for instances of physical threats towards the PSU.[32] In Denmark the ADR practice is akin to the situation in Sweden, but this is being challenged in scholarship and in the court system.[33]

9. Also in the Netherlands the distinction between authorised and unauthorised payments is not clear. For example, in a case with the Dutch Institute for Financial Disputes the ADR body in first instance concluded that a transaction was authorised, because the PSU had himself authenticated the transactions, whereas the appellate body considered the transactions unauthorised, because the PSU did not have the intent to transfer any funds but was tricked into doing so by the fraudster.[34]

2.3 The interplay between PSD2 and liability for APP fraud based on national law

10. Whereas in PSD2, liability for unauthorised transactions is allocated to the PSP, for APP fraud the PSD2 rules are not clear. There are two main streams of thinking. Some countries, based on jurisprudence of the European Court of Justice, are of the view that PSD2 implies that a PSP can never be held liable for authorised transactions. Some other countries believe that PSD2 is, in essence, silent on authorised transactions and that therefore the national private law, which often means the PSP's general duty of care, applies. We illustrate this below by explaining the Belgian and Dutch position.

11. In Belgium, the prevailing view in literature is that a PSP cannot be held liable if it executed a fraudulent, but authorised, payment order in accordance with the unique identifier provided by the payer.[35] This view was also upheld by the commercial court in Antwerp stating that the liability regime in the Act on Payments Services, at that time

---

30 Finkn-2020-490, FinKN 2022-684, FinKN-2022-978 og FinKN-2023-355, FinKN-2023-664.

31 FinKN-2024-309.

32 M.R. Aagaard, 'Tredjemans svikliga förledande – Kan en godkänd betalningstransaktion vara obehörig?', *SVJT* 2024(5), p 323.

33 S. Karstoft, 'Forbrugeres hæftelse for netbankoverførsler som følge af bedrageriske telefonopkald', *Erhvervsjuridisk Tidsskrift* 2024, pp 99-100. Copenhagen City Court case BS-28021/2023-KBH (ongoing).

34 Dutch Institute for Financial Disputes 17 January 2023, 2023-0042, https://www.kifid.nl/Uitspraak-2023-0042-Bindend.pdf and Decision of the Appelate Body of the Dutch Institute for Financial Disputes 4 September 2023, 2023-0036, https://www.kifid.nl//2023/09/Uitspraak-2023-0036.pdf.

35 J.P. Buyle and O. Piret-Gerard, 'Le devoir du vigilance du prestataire de service de paiement ou la tentation du sophisme', in J. Sad, *Les services de paiement en droit belge*, Anthémis (Antwerp : Anthemis, 2024), pp161-188 ; D. Blommaert, L. Van Muylem and A. Guillaume, 'Responsabilité des prestataires de services de paiement : application exclusive du régime spécifique du Code de droit économique et exclusion de la responsabilité de droit commun', *TBH* (*Revue de Droit Commercia)* 2025 (to be published) and O. Creplet, 'Ordre de virement falsifié: le point sur l'ancienne controverse, spécialement depuis l'entrée en vigueur de la loi relative aux services de paiement', *TBH* (*Revue de droit commercial)* 2013, p 597.

transposing PSD1, governs liability conclusively.[36] More recently, the commercial court in Brussels refused to impose liability on the PSP on the basis of a violation of the general duty of care, arguing PSD2 does not allow this.[37] More specifically, the court referred to the case law of the European Court of Justice, stating that both a parallel liability regime in respect of the same operative event and a competing liability regime allowing the PSU to trigger that liability on the basis of other events, are incompatible with the full harmonisation approach of PSD2.[38] Remarkably, a different chamber of the same commercial court decided otherwise, and applied the general duty of care to conclude to joint liability.[39] However, this latter decision is at the moment subject to appeal. This interpretation commonly held in Belgium seems at odds with the view of the EC who earlier stated that PSD2 "does not cover the types of fraud which have emerged since its adoption and which have become increasingly widespread, such as cases where consumers are manipulated by fraudsters and tricked into authorising a payment transaction (so-called 'authorised push payments' fraud)", but this view by the EC was delivered before the European Court of Justice issued its decision and it is up to the European Court of Justice to authoritatively interpret EU law.[40]

12. In the Netherlands, there have been many cases where the victim (the PSU) of APP fraud invoked the general duty of care of the PSP.[41] The victim has rarely been successful so far, but in the Netherlands there is not a legal bar against this form of liability, as opposed to the Belgian position discussed above.[42] Such claims invoking a special duty of care are

---

36 Commercial Court Antwerp (Hasselt) 24 June 2015, *DAOR* 2015, no. 116, 138.

37 Commercial Court Brussels 28 August 2024, *Revue de droit commercial* 2024 (to be published).

38 See European Court of Justice 11 July 2024, *UA / Eurobank Bulgaria,* ECLI:EU:C:2024:600, no. 57-59, https://eur-lex.europa.eu and European Court of Justice 2 September 2021, *CRCAM / France*, ECLI:EU:C:2021:671, 52, https://curia.europa.eu. A similar view, but with regard to unauthorised payments can be found in a judgement of the Court of First Instance of Brussels of 4 January 2024, *Droit Bancaire et Financier* 2024/2, 1.

39 Commercial Court Brussels 30 November 2023, *Droit Bancaire et Financier* 2024/3, 1.

40 See answer given by Ms McGuinness on behalf of the European Commission 4 May 2023, available here https://www.europarl.europa.eu/doceo/document/E-9-2023-000775-ASW_EN.html.

41 Gerechtshof Arnhem-Leeuwarden 24 December 2024,https://uitspraken.rechtspraak.nl/ECLI:NL:GHARL:2024:7950, Rechtbank Amsterdam 23 January 2024, https://uitspraken.rechtspraak.nl/ECLI:NL:RBAMS:2024:441, ,Rechtbank Amsterdam 20 November 2024, https://uitspraken.rechtspraak.nl/ECLI:NL:RBAMS:2024:7070E, https://uitspraken.rechtspraak.nl/; Dutch Institute for Financial Disputes 4 February 2025, 2025-088, https://www.kifid.nl/2025/02/Uitspraak-2025-0088.

42 Also somewhat in this direction, Norwegian Supreme Court case 2024-990-A, https://www.domstol.no In the UK, the applicability of the so-called Quincecare duty was tested and established in *Barclays Bank plc v Quincecare Ltd [1992] 4 All ER 363*. According to this, the bank has to refuse to honour the customers' transaction if they have reasonable grounds (although not necessarily proof) for believing that the payment instruction was an attempt to commit fraud. This duty was tested in *Philipp v Barclays Bank UK plc [2023] UKSC 25*, where the court ruled that the Quincecare duty does not apply to situations where the payment instruction was coming from the customer. In the Quincecare case and subsequent cases where the duty was upheld, the customer was defrauded by their agent, for example, the company director or a partner in the law firm. The duty was again raised in the *Larsson v Revolut Ltd [2024] EWHC 1287 (Ch), w*here Revolut was the receiving and not the sending institution. The court held, however, that the Quincecare duty of care does not extend to third parties.

rarely successful though, because PSPs are not expected to monitor transactions – except, of course, to combat money laundering[43] – or to assess their technical correctness. One can doubt whether this is correct as there are several legal documents pursuant to PSD2 pointing towards the opposite conclusion,[44] but this this is how all Dutch courts and ADR bodies currently see this. Only if the PSP receives signals that something is wrong for other reasons, which is hardly ever the case, they must intervene based on their duty of care.[45] Once alerted, the PSP must investigate in the interest of the potentially harmed payers whether there is fraud. For the recognition of a breach of duty of care, subjective knowledge is required from (employees of) the PSP regarding the unusual course of transactions in the account of the PSU. The threshold is: did the PSP actually know that something was wrong? In those rare cases that the PSU was successful, the PSU himself reported that he was a victim of APP fraud, but the PSP did not act swiftly to prevent further damage, for example by blocking the account for in case the fraudster contacted the PSU again.[46] Interestingly, in the Dutch jurisprudence as opposed to Belgium, it was never discussed whether EU law allows for such a ground of liability next to PSD2. So it was not that the Dutch courts explicitly interpreted the case law of the European Court of Justice or PSD2 differently; so far the Dutch courts did not even discuss this.

2.4 The applicability of the general private law principle of lack of consent based on fraud, deception or mental disorder

13. It should be noted that in many of these cases, there was also a defect of consent on the part of the PSU, for example due to induced mistake, fraud, coercion, or unfair exploitation

---

See also, in Portugal, Sentence of *Tribunal da Relação de Lisboa* of 20 February 2024 (Rapporteur Rute Lopes), stating that the PSP has a duty to protect the clients' money based on good faith because it has the means to equip itself with the most advanced technological means to detect whether the security of the instrument has been compromised. The Court considered that something went wrong with the bank's security system, which, equipped and managed by sophisticated algorithms, failed to detect in the space of 87 minutes, 25 transactions (one every 3.5 minutes), and to consider the possibility that part of those could actually be the result of intrusive and fraudulent use. This position was already adopted by Portuguese appeal courts before the transposition of PSD2: see Sentence of *Tribunal da Relação de Évora* of 22 May 2014 (Rapporteur Mata Ribeiro) and Sentence of *Tribunal da Relação de Guimarães* of 17 December 2014 (Rapporteur Fernando Fernandes Freitas).

[43] According to Dutch case law, the violation of anti-money laundering legislation has (at least in principle) no private law consequences. See for example Rechtbank Amsterdam 22 January 2025, https://uitspraken.rechtspraak.nl/ECLI:NL:RBAMS:2025:404 and Rechtbank Zeeland-West-Brabant 8 May 2024, https://uitspraken.rechtspraak.nl/ECLI:NL:RBZWB:2024:7554.

[44] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, article 2. EBA Final Report Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2), EBA/GL/2018/05 (consolidated version), 18 July 2018, p. 16, https://eur-lex.europa.eu/eli/reg_del/2018/389/oj/eng.

[45] See for example Rechtbank Amsterdam 14 May 2018, , https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2018:2984 and Dutch Institute for Financial Disputes 4 November 2024, 2024-0954, https://www.kifid.nl.

[46] See Gerechtshof Arnhem-Leeuwarden 24 December 2024, , https://uitspraken.rechtspraak.nl/ECLI:NL:GHARL:2024:7950 and Gerechtshof Amsterdam 29 March 2022, 0, https://uitspraken.rechtspraak.nl/ECLI:NL:GHAMS:2022:940 and Dutch Institute for Financial Disputes 17 January 2025, 2025-0018, https://www.kifid.nl/wp-content/uploads/2025/03/Voorzittersbeslissing-2025-0024.pdf.

by the fraudster. However, it is questionable, both from an EU law perspective and from a private law perspective, whether the PSU can rely on defects of consent when making a PSD2-claim against his PSP. Firstly, provided that national private law would allow for the invocation of these defects of consent against the PSP, one could ask whether this application of national private law rules would be in conformity with PSD2, which at least aims for maximum harmonisation for unauthorised transactions. When the future PSR would also fully harmonise (some forms of) authorised push payments, the scope for a claim based on lack of consent would be even more limited. Secondly, even from a purely private law perspective, it is unclear whether these grounds of invalidity (induced by the fraudster) can be invoked against a third party who was unaware of them, such as the PSP.[47],[48] It is telling that both the European Draft Common Frame of Reference (DCFR, article II-7:208 par. 2) and the Principles of European Contract Law (PECL, 4:111 par. 2) both require that the third party was or should have been aware of the relevant facts, i.e. of the fraud. With an automated process like the execution of (mass retail) payments, factual or objective knowledge of fraud on the part of the PSP could only result from an obligation to monitor for potentially fraudulent transactions and a duty to act on this. The question whether or not a bank can be held liable for a defect of consent on the part of the PSU, caused by the fraudster, therefore boils down to the same question as the one we discussed above in 2.3, namely whether and to what extent the PSP owes duty of care to monitor transactions and act upon signals of fraud.

3. Liability for PSPs beyond bank impersonation fraud?

14. As indicated in the introduction, the PSR proposal suggests a liability shift for APP fraud, but only in case of bank impersonation fraud. In the EP's position, it was suggested that PSPs should be liable in all cases of impersonation fraud, regardless of whom the fraudster was impersonating.[49] The EP refers to impersonation of the consumer's PSP *or any other relevant entity of a public or private nature*. Such a wider liability for APP fraud has, for example, been introduced in the UK.[50] The first key question, therefore, is whether it should matter for the assumption of liability who the fraudster is impersonating.

3.1 Distinguishing between types of fraud: trust in who is at stake

---

47 Article 3:44 and 3:35 Dutch Civil Code.

48 In Denmark, the leading literature assumes that authorisation is subject to national contractual rules on mistake etc., see Karstoft 2024. In Sweden, a quite detailed analysis by Rødvei Aagaard 2024 argues the opposite.

49 *European Parliament legislative resolution on the proposal for a regulation of the European parliament and of the Council on payment services in it the internal market and amending Regulation (EU) No 1093/2010*, 23 april 2024, T9-0298/2024 on art. 59 sub 1, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0298.

50 Payment Systems Regulator, Specific Direction 20 (Faster Payments APP scam reimbursement requirement), December 2023 at https://www.psr.org.uk/media/zhkp0vbt/specific-direction-20-reimbursement-requirement-to-directed-psps-dec-2023.pdf. The new rules apply to all types of authorised push payment scam which means using a fraudulent or dishonest act or course of conduct to manipulate, deceive or persuade a consumer into transferring funds from the consumer's relevant account to a relevant account not controlled by the consumer, where the recipient is not who the consumer intended to pay, or the payment is not for the purpose the consumer intended See extensively on the background to the new rules J. Braithwaite, 'Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like, *JFR 2024*, , pp 1–20.

15. The majority of the authors of this paper are of the view that APP fraud which can be traced back to abusing peoples' trust in the payment system (for example impersonation of the police, regulator or government) justifies liability of the PSP. In the case law, we have seen many organisations and natural persons having been impersonated, but all with a view towards convincing the client to take action to keep his funds at the PSP safe. A telling example was a claim at the Dutch Institute for Financial Disputes where the fraudster was not impersonating the PSP but the Dutch Central Bank,[51] and the famous UK Philip v Barclays-case where the fraudster was impersonating the Financial Conduct Authority.[52] Our view is that peoples' trust in the payment system must be protected by means of a compensation mechanism in case of such fraud scenarios, because otherwise PSUs may withdraw from using banking services entirely.

16. There are however, also all kind of unfortunate cases that cannot be traced back to abusing peoples' trust in the financial system. Fraudsters could impersonate practically anyone. In the case law we have seen fraudster impersonate a military in Iraq (a case of love fraud), family members (such is often the case in WhatsApp fraud), and genuine investment opportunities (which is the case in so called pig-butchering scams). In essence it is not the credibility of financial services that is at stake, but of (people you meet through) social media. There are also fraudsters that do not impersonate, but still manage to successfully commit fraud. For example in a case for the Dutch Institute for Financial Disputes an elderly man was deceived by his son-in-law.[53] It was not disputed that this person had married his daughter, but the fraud was that he tricked his father-in-law into making payments to his own bank account. No matter how repulsive, in these cases of elderly abuse it is not the credibility of modern banking that is at stake. Next to the cases of APP fraud discussed above, we have seen other cases where the PSU alleges that the PSP should have monitored his payment behaviour. These cases can be summarised as "not fraud, still unfortunate". A Dutch example concerns a student that blew through the entire savings account with a balance of €32,400 within less than a months with gambling.[54] The student tried to blame this on the PSP stating that because of the general duty of care, the PSP should have prevented this. The Dutch Institute for Financial Disputes rejected this claim.

17. Whether PSPs have a role to play in protecting PSUs against these other ills of society, is in our view less obvious as it leans (too) much towards paternalism. One specific case though, which we discuss in paragraph 3.6*, is invoice fraud, also referred to as name number fraud. As we will see here the EU legislator has already provided for specific rules to combat this type of fraud.

3.2 Grounds in favour of extended liability for APP fraud that can be traced back to abusing peoples' trust in the payment system

---

51 Dutch Institute for Financial Disputes 21 November 2023, 2023-0878, https://www.kifid.nl/wp-content/uploads/2023/11/Uitspraak-2023-0878.

52 The Supreme Court of the United Kingdom 12 July 2023, *Philipp (Respondent) v Barclays Bank UK PLC (Appellant)*, https://www.supremecourt.uk/cases/uksc-2022-0075.

53 Appelate Body of the Dutch Institute for Financial Disputes 1 May 2019, 2020-027, https://www.kifid.nl/wp-content/uploads/2023/09/Uitspraak-2023-0036.

54 Dutch Institute for Financial Disputes 26 October 2018, 2018-675, https://www.kifid.nl/wp-content/uploads/2018/11/Uitspraak-2018-675.

In our view, there are several grounds in favour of liability of PSPs in case of APP fraud that only apply in case of fraud which can be traced back to abusing peoples' trust in the financial system, but do not support allocating fraud to PSPs in other cases.

18. Firstly, a general societal interest in placing the risk of fraud with the PSPs, would be to maintain trust in digital payment methods.[55] If PSUs were to become widespread fearful of falling victim to APP fraud and did not trust that they would be compensated, this could lead to a decline in confidence in the digital payment system. However, the relevance of this consideration varies depending on the type of fraud scenario. With bank impersonation fraud the fear is, in essence, that funds are not safe with the bank. This fear is caused by the complexity of modern banking and should not result in bank withdrawals by PSUs.

However, with other fraud scenarios, other complexities of society are exploited. For instance, relationship fraud and fake advertisements at market places may be linked to online/social media in general. We are sceptical whether the trust in these kinds of people or organisations should be strengthened via compensation mechanisms by PSPs. Perhaps people should learn that (others you meet on) social media are not to be trusted. Also, if social media should be trusted, it is principally these social media that should take measures to warrant this trust. In the EP's version of PSR, significant effort is required from social media and telecommunication providers.[56]

19. Secondly, it is primarily the PSPs that have promoted digital payment methods and encouraged their PSUs to use these modern tools. Other, less modern methods of paying are discouraged by most PSP. This also points towards allocating the risks that are specifically caused by the use of these digital payment methods with PSPs. Put differently: if the financial industry invents the possibility for PSUs to authorise transactions with their smartphone, this automatically means that this is a new avenue for fraud. Therefore, there are compelling reasons in allocating liability with the inventors of this new avenue for fraud as well.

20. Thirdly, digital banking has significantly reduced risks for banks in the physical storing and transporting of cash. Whereas the consequences of physical bank robberies were borne by the bank, the risk of online fraud without further legislative intervention will be borne by the PSU. This was one of the reasons to allocate the risk of unauthorised fraud to the PSPs in PSD1. Quoting the impact assessment accompanying the PSD1 proposal:[57] "*Whereas the classic bank robbery of the past involved the appropriation of gold or bank notes belonging to the bank (rather than specific customers), bank crime in the electronic age involves the unauthorised withdrawal of credit from the accounts of specific customers. Rather than the losses associated with bank crime being borne by the bank (i.e. bank customers and bank shareholders collectively) remote banking gives rise to the possibility of significant losses being*

---

55 See also Dir. 2015/2366 recital (69) where it is made explicit tath the political choice has been made to allocate liability for unauthorised transactions with the PSP, to ensure that consumers are willing to use the services of PSPs.

56 See article 59 PSR, Decision by Parliament, 1st reading voted upon 23 April 2024, T9-0298/2024.

57 See Commission staff working document - *Annex to the proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market - Impact assessment* 1 December 2005, *{COM(2005) 603 final} /* SEC/2005/1535 */ section 6.1,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005SC1535.

borne by a few individual consumers. To state blithely that electronic forms of banking have fewer security risks associated with them than cash banking is to miss the point. If and when the security risks materialise consumers using remote banking services can have their accounts emptied or even be forced into debt. It is the consequence of the risks associated with remote banking rather than the level of the risks that is of most concern to consumers. There is also an important point of principle at stake. Banks are in the business of providing security. It is therefore them, rather than the individual consumer who should bear the loss if criminals find ways around banking security systems."

3.3 Grounds in favour of extended liability for APP for all fraud

The considerations below support a wider application of a liability for APP fraud, also for cases that cannot be traced back to abusing peoples' trust in the financial system.

21. Firstly, liability for APP fraud can be seen as a kind of insurance for the PSU. All PSUs face the risk of becoming victims of fraud. For the individual PSU, this is a significant problem, as it could involve a significant portion of their wealth. However, PSUs cannot insure themselves against this risk – as far as we know, no insurer offers such insurance. By having the PSP cover the risk, PSUs are effectively insured. However, PSPs may increase prices for all their PSUs by slightly increasing the service fees for all PSUs to cover for all fraud related reimbursements. It also our impression that the amounts stolen via APP fraud have become much more significant over time than unauthorised fraud always used to be, which necessitates this extended risk sharing also for APP fraud.

22. Secondly, PSPs are better placed to fight payment fraud via advanced monitoring mechanisms than the PSUs themselves.[58] PSPs will have more incentives to combat APP fraud if they are required to compensate the victim. This may prompt them to invest more in systems to prevent fraud, such as improved monitoring. They can then assess for themselves what is more economically optimal: investing more in combating APP fraud, or accepting the risk that their PSUs are more frequently victims of fraud and the PSP has to then compensate them.[59] It was the same idea that led the EU co-legislators to make PSPs liable for unauthorised payments in PSD1, namely to incentivize PSPs to invest in the security of payments instruments. Quoting the impact assessment accompanying the PSD1 proposal: *"In this respect it has to be considered what impact the legal provisions may have on the incentives of the contractual parties to fulfil their respective safekeeping obligations."*[60]

This also is in line with general private law ideas. If it becomes easier and cheaper to monitor clients' payment behaviour, PSPs are increasingly expected to do so. This follows directly from the well-known Dutch *Kelderluik* ruling, which basically says that if someone creates a dangerous situation, where someone less diligent is exposed to the risk of significant harm, the former person must take measures to manage the risk. The lower the level of effort

---

58 See for example the Which? super-complaint Consumer safeguards in the market for push payments, 23 September 2016, where this argument was well developed. Available here https://www.psr.org.uk/media/t0sln5vn/which-super-complaint-sep-2016.pdf.

59 Another reason for a PSP to invest in better fraud monitoring is to be able to apply more exemptions to the SCA requirement, leading to a better customer journey for the PSU.

60 See Commission staff working document - Annex to the proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market - Impact assessment {COM(2005) 603 final} /* SEC/2005/1535 */ section 6.1.

required, the more measures are expected.[61] From this, we infer that if it becomes cheaper (and thus less burdensome) due to technological advancements to monitor payment accounts, PSPs are more likely to be expected to actively monitor payment behaviour. Additionally, a PSP must keep up with the state of the art. This consideration can be found in a case of the Dutch Institute for Financial Disputes, where the Dutch Institute for Financial Disputes evaluated whether a PSP that is lagging in safety measures as compared to competitors in the market should be held liable for that reason.[62] In this specific case the Dutch Institute for Financial Disputes ruled that the PSP was not that much behind that it led to liability on their side.

23. Thirdly, It would relieve the PSU from the problematic position of having to prove that the PSP performed insufficient in monitoring potential fraudulent transactions. As explained above in section 2.3, the current position in many countries is that victims must prove the subjective knowledge of the PSP that fraud may have occurred or have to prove the inadequacy of the PSP's fraud monitoring process. This is a burdensome position for PSUs, as they cannot investigate and evaluate the PSP's fraud monitoring mechanisms. The fact that PSUs do not really understand how PSPs monitor their accounts is beneficial as well, as it also prevents criminals from familiarising themselves with PSPs' monitoring mechanisms.[63] A risk-based liability allocated with the PSP for (specific types of) APP fraud would resolve this complicated situation where PSUs are required to prove something they cannot prove. As an alternative, the co-legislator (or regulator) could at least prescribe what is minimally expected from PSPs in terms of fraud monitoring, which indeed seems to be the case now in PSR, although still defined at an abstract level (see section 4.2*). The PSU would then only need to prove that if the PSP monitored according to the requirements and would have taken action, the PSU would not have been a victim of APP fraud.

24. Lastly, the current difference in treatment between unauthorised payments and APP fraud is often unfair, since an equally gullible victim in a highly comparable situation sometimes does and sometimes does not get compensated, depending on the modus operandi of the fraudster. We explain by comparing two slightly different fraud scenarios. In case A, the PSU's bank card and PIN (or other personalised security credentials) are obtained through deceit and fraud. In this situation, the PSP must compensate the PSU for the loss, unless the PSU was grossly negligent. In other words, if the PSU was particularly careless to fall for the deception. In case B, the PSU is tricked into transferring money themselves in order to keep the money safe. In this case, the PSU's own fault is not relevant. What matters is whether the PSP knew something was wrong and should have investigated further based on his duty of care. Although the PSU is also deceived in case B and might even have been less gullible than in case A, the PSU in most EU jurisdictions still has to bear the full loss in

---

61 Hoge Raad der Nederlanden 5 November 1965, *Kelderluik,* Dutch Supreme Court 5 November 1965, https://uitspraken.rechtspraak.nl/ECLI:NL:HR:1965:AB7079 = *NJ 1966/136*.

62 Dutch Institute for Financial Disputes 19 January 2018, 2018-670, https://www.kifid.nl/media/cj4kmgeb/uitspraak-2018-670-bindend-pdf.pdf.

63 For that reason Dutch courts have held that PSPs are not obliged to give insight into how their monitoring systems work Rechtbank Amsterdam 19 July 2023, ECLI:NL:RBAMS:2023:4597, no. 3.4, https://uitspraken.rechtspraak.nl/ECLI:NL:RBAMS:2023:4597. This has also been a theme in Norwegian litigation, see LB-2021-53168 from Borgarting Court of Appeals.

case B. Introducing a liability for the PSP in case of APP fraud that can be traced back to abusing peoples' trust in the payment system remedies this situation.

3.4 Grounds against extended liability for APP fraud.

Arguments can also be made against allocating liability for APP fraud with PSPs. These grounds apply also to cases that can be traced back to abusing peoples' trust in the financial system.

25. Firstly, the fundamental question can be raised whether the loss, which was neither caused by the PSP or the PSUs (but by the fraudster), should be carried by the PSPs or by the PSUs. Some fear that PSUs may be less cautious, if they know they will get compensated. This is the moral hazard argument. Then the PSPs may increase the prices for their services to all PSUs, to compensate for the additional costs because of fraud. In our view, however, we consider it rather unlikely for this moral hazard argument to apply in practice in most fraud scenarios. Even though victims may get compensated after all, being defrauded of a substantial part of one's savings is a traumatic experience and it is not certain beforehand, whether the PSPs will indeed compensate in such cases. Furthermore, applying for reimbursement can take a long time and involve a laborious process. One should also not overestimate the degree to which PSUs, especially consumers, adapt their behaviour to this kind of technical legislation. Therefore, in general we do not fear that PSUs will become less diligent. Only in some fraud scenarios some moral hazard risk may be realistic, for example PSUs may be less diligent when ordering goods online, when they know that they will be reimbursed in case the good they bought did not get delivered.[64]

26. Secondly, the question arises whether risk-sharing between PSUs is desirable. As explained in 3.3, risk liability of PSPs functions as a *de facto* mandatory insurance against fraud. Because of this liability, PSPs will likely be incentivised to invest more in combatting fraud. These costs will probably be spread out over all PSUs. Although in principle anyone can become a victim of this fraud, there are PSUs who may be less susceptible. They may be less inclined to appreciate such enforced solidarity with more vulnerable PSUs. "Why should I pay for someone else who becomes a victim of fraud?" they may ask. The answer to this question is in the end deeply political and depends on the type of society we want to build. Of course this argument is less strong when the fees charged by the PSP would already reflect the higher risk of liability, for example when PSPs would charge more to PSUs with a higher balance (that can be defrauded).

27. Thirdly, the risk of fraudulent claims may increase. Someone could always claim to be a victim of APP fraud in order to receive compensation, even if this was not the case. Consider someone who claims to be a victim of relationship fraud and, for that reason, transferred money abroad, but was actually in cahoots with the fraudster and simply received the money back in cash. Such fraud is not exclusive to payments. How many people claim to have lost their sunglasses with their insurance company, only to be seen wearing them in photos on

---

64 Also the overall framework of EU consumer protection is built on the idea that consumers need protection and many of these rules will to some extent create moral hazard. For example the fact that a consumer can send back a product when it does not meet his expectations, could lead consumers to be less diligent when ordering something in the first place. Still this rule has been introduced in Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, article 9.

social media? The same risk exists with unauthorised transactions. The more grounds for liability, the more opportunity for fraudulent claims.

28. Lastly, when PSPs are going to be held liable, they will also have a legitimate interest in monitoring the PSUs payments behaviour. By some PSUs, this could be experienced as overly intrusive, especially when monitoring is based on AI and profiling as suggested in the PSR (see section 4.2). Also when PSPs are going to be held liable, they will want to act to manage their liabilities. Except for just monitoring they will also need to be able to take action, for example by warning PSUs, and suspending transactions or even blocking transactions (to be discussed in more detail in section 4.4 and 4.5). As we explain in more detail there, for some fraud scenarios this would be particularly invasive and paternalistic, which also argues against imposing liability on PSPs for these fraud scenarios.

3.5 Distinction consumer versus professional

29. Under PSD2 for non-consumer PSUs, less favourable liability rules may be agreed upon in the framework contract between PSU and PSP for unauthorised transactions.[65],[66] This is justified in the recital to PSD2 as follows: "*Provision should be made for the allocation of losses in the case of unauthorised payment transactions. Different provisions may apply to payment service users who are not consumers, since such users are normally in a better position to assess the risk of fraud and take countervailing measures.*" We consider this a reasonable approach for APP fraud as well. The key argument for this is that corporates should also have their own processes for fighting fraud. For example, when it is an employee defrauding the company, the bar for liability should be much higher, because you want companies to organise themselves in such a way that this kind of fraud is not possible. In the same vein, in case of CEO fraud, the company itself can manage this risk by having good internal authorisation processes for any payment (such as the 4-eyes principle).[67]

3.6 The specific case of invoice fraud (verification of payee)

30. An APP fraud scenario that already has gotten specific attention of the EU legislator is invoice fraud, or the more generic concept of name-number fraud. Next to the IBAN, PSUs often also provide the name of the payee in their payment order. Based on the rules of PSD2 PSPs only use the IBAN when executing payments and do not pay attention to the name mentioned by the payer. There is a good reason for this, as names may be spelled in different ways. It would interfere with the objective of smooth and fast payments when transactions would be suspended when the name does not match. The European Court of Justice ruled that both the PSP of the payer and the PSP of the payee are not liable, if they only use the

---

65 Article 61 sub 1 Dir. 2015/2366.

66 Article 27 PSR provides for the same rules.

67 The UK has introduced a liability cap for PSPs. Specific Requirement 1 in para. 4.4. providing that the PRS sets the cap and publishes it on its website. The limit is currently £85.000 which aligned with the Financial Services Compensation Scheme's amount for failed companies. If consumers are reimbursed above the cap, that will be considered voluntary reimbursement under para. 5.18 and is considered to be outside the scope of the PSR reimbursement rules under para. 5.19. See https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protectionsThe EU could consider this as well to tailor the compensation rights towards retail PSUs and the amount they typically deal with, as corporates should protect themselves.

IBAN and do not check whether the name of the payee and the IBAN match.[68] On the other hand, based on the grounds discussed above there is also something to say in favour of liability, because checking whether the account belongs to the named individual is technically feasible and does not bring along many of the grounds against liability listed in 3.4 and further. The EU legislator has come up with a compromise, requiring the PSP of the payer to provide a verification of payee. Basically, the PSP must warn the PSP if name and number do not fully match, but it is then for the payer to determine whether to move ahead anyhow or refrain from this transaction.[69]

4. Defining what PSPs can do when combating fraud: balancing safety with privacy and autonomy of the PSU

When PSPs are going to be held liable they will want to be able to manage their liabilities. This is also the purpose of the EU co-legislator, as it wants to bring down payment fraud and wants to incentivise PSPs to put effort into this. In our view, the EU co-legislator should consider what PSPs can do to manage their liability risk, because this can also become overly intrusive. We explain the options accompanied with the pros and cons.

4.1 Educating and alerting PSUs about general fraud risks

31. Firstly, PSPs could be involved in campaigns raising awareness of the risk of fraud and the modus operandi of fraudsters. PSPs can do this jointly, for example by television campaigns or directly towards their own PSUs. Apart from the costs involved, there seems to be no downside to this. PSR also introduces a requirement to this extent.[70] Of course, one might wonder whether financial education should be a task of the private sector or of the public sector/the regulator, but it seems PSR has chosen the former.[71]

4.2 Monitoring for fraud in transactions

32. As a next step, PSPs may also want to monitor the transactions of their PSUs for fraudulent transactions. This exactly what is expected of them per the proposals of PSR. PSR considers the timely detection of fraudulent transactions essential, and considers that transaction monitoring plays an import role in that detection.[72] PSPs must therefore have in place transaction monitoring mechanisms.[73] These transaction monitoring mechanisms have as their purpose, amongst others, to enable PSPs to prevent and detect potentially fraudulent transactions. PSR also specifies what needs to be done. Notably the transaction

---

68 European Court of Justice 21 March 2019, C-245/18.

69 Article 5c Regulation as regards instant credit transfers in euro (IPR), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202400886.

70 Article 84 PSR.

71 See for example Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property, article 6 where financial education is designated as a task for the member states, https://eur-lex.europa.eu/eli/dir/2014/17/oj/eng. See also the proposal for an update of MiFID II in the Retail Investment Strategy Proposal for a Directive of the European Parliament and of the Council amending Directives (EU) 2009/65/EC, 2009/138/EC, 2011/61/EU, 2014/65/EU and (EU) 2016/97 as regards the Union retail investor protection rules, 7 June 2024, COD 2023/0167, article 16a, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0279.

72 PSR recital (100).

73 Article 83 sub 1 and sub 2 PSR.

monitoring mechanisms shall also be based on the analysis of previous transactions and access to payment accounts online. Also, PSPs are called upon in the recitals to use artificial intelligence to keep on par with the fraudsters.[74] So the idea is that also PSU specific data is used for the transaction monitoring (such as environmental and behavioural characteristics and transaction history of the PSU) next to more generic data (such as the amount of the transaction and known fraud scenarios).

Naturally, this will infringe on the privacy of clients, as it will involve large scale data processing to look for fraudulent transactions. Therefore, the co-legislators need to be mindful when imposing or authorising new monitoring roles on PSPs. Some authors of this paper would rather have increased service fees to act as a *de facto* insurance for APP fraud, than increased transaction monitoring.

4.3 Warning the PSU for a concrete transaction

33. Monitoring is of course only useful, if PSPs can act upon their findings. This is where it gets tricky. The most logical step for PSPs is to contact their PSU in case of suspicions of fraud. This is already common practice in the context of the efforts of PSPs to combat unauthorised transactions. For example, PSPs contact their PSU when their bank card is used within a short period of time over a large geographical distance. Normally when monitoring for fraud with unauthorised transactions, the only question when contacted is whether the PSU indeed authenticated this specific transaction.

However, with APP fraud the situation can be complicated. In case of suspected bank impersonation fraud, it means warning the PSU that he is the victim of fraud and verifying with the PSU whether he wants this transaction. It is quite likely that the PSU is under the "spell" of the fraudster, which means a tough conversation for the PSP with the PSU.[75]

For some fraud scenarios the discussion is even more complicated. For example, when the PSP thinks the PSU is a victim of relationship fraud, the PSP needs to discuss with the PSU the nature of this possibly fake relationship. Some people may not like discussing the nature of their romantic relationships with their PSP. And if the PSU is cheating he may really not like discussing this relationship with the PSP in front of his significant other. Even engaging in a romantic relationship which turns out to be fictitious, may still not go down well with one's spouse. Basically, taking action when the PSU is a victim of APP fraud often requires a much more privacy-intrusive action by the PSP, then in case of unauthorised transactions. The fact that the action to be taken by the PSP is so complex, could be a reason not to allocate liability with the PSP for these kind of fraud scenarios.

4.4 Suspending a concrete transaction or cooling off periods

34. For some fraud scenarios, warning a PSU is only effective if the PSP can at least suspend the transaction. Suspending transactions, which is the only credible way of fighting bank impersonation fraud which only happens within the timeframe of a day, even if allowed for under the contract with the PSU, may be at odds with the Instant Payments Regulation

---

74 PSR recital (103).

75 See for example Appelate Body of the Dutch Institute for Financial Disputes 7 February 2025, 2025-0012, https://www.kifid.nl/media/iiihl1mw/uitspraak-2025-0012-pdf.pdf, where the PSP after an internal alert did call the PSU to enquire whether he was a victim of bank impersonation fraud, but the fraudster managed to instruct the PSU to lie to the real bank.

which requires that instant credit transfers are executed instantly. The EC in its Q&A suggested that the question whether blocking an instant credit transfer because of suspicions of fraud is allowed, would need to be dealt with in PSR.[76] An alternative is to apply a cooling off period for large transactions, meaning that transactions above a certain threshold would not be executed instantaneously, but after some hours or even days. This also seems at odds with the Instant Payments Regulation,[77] but would be allowed when transferring amounts from the savings account (which is not in scope of the Instant Payments Regulation) to the current account.

35. We believe that the PSP should not be held liable for blocking a transaction or warning the PSU when it has reasonable grounds for believing that the PSU may be a victim of fraud. For example, we have seen a, albeit relatively rare, case where the PSU actually brought proceedings against his PSP for suspending a transaction, when the PSP had concerns of WhatsApp fraud.[78] This is comparable to the situation where a financial institution suspends a transaction when it is concerned it may otherwise breach sanction laws. In such instance a financial institution cannot be held liable, even if the financial institution turned out to be incorrect.[79]

36. The Instant Payments Regulation enables the possibility of setting a maximum limit that can be sent by means of instant credit transfer.[80] Banks could set a low default limit in order to protect PSUs and reach out when the PSU increases the limit. However, according to the EC, the PSU should be able to opt out from such contractually agreed cooling-off period without difficulty and with immediate effect.[81]

37. We suggest a more critical stance towards the Instant Payments Regulation, when it concerns large value payments for consumers. Generally, consumers do not need instant payments when making large payments and usually know well in advance when they need to make such larger payments. Some fraud scenarios develop gradually over time, such as pig butchering scams and relationship fraud. Suspension of a specific transaction would then not be required to serve the desired effects.

4.5 No blocking of transactions and no escalation towards family

---

76 See the EC Q&As on IPR implementation, Q&A 90, https://finance.ec.europa.eu/document/download/f597b1a5-2a7b-481d-882c-80fb1c5cc3d5_en?.

77 Article 5a IPR.

78 Dutch Institute for Financial Disputes 2023-0078, https://www.kifid.nl/wp-content/uploads/2023/02/Uitspraak-2023-0078 similarly from Norway FinKN 2024-714, https://publisering.finkn.no/statement/2024-714.

79 Article 10 sub 1 Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine.

80 Article 5c IPR.

81 See the EC Q&As on IPR implementation, Q&A 68, https://finance.ec.europa.eu/document/download/f597b1a5-2a7b-481d-882c-80fb1c5cc3d5_en?.

38. Some PSUs may not believe their PSP, even when being warned by their PSP. Sometimes the spell of the fraudster is that strong.[82] Banks may then feel obliged to reach out to family of the victim -with even more privacy concerns- or may want to block the transactions. By way of illustration, in Singapore it is now proposed by way of law that the police should be able to block transactions, because some victims even after being warned by the police continue to transfer funds to the fraudster.[83] Although we understand the desire to help obviously irrational people when acting against their own interest, we consider such an approach inappropriate from a European private law perspective. The principle of autonomy lies at the heart of European private law. Consequently, contracting parties bear the risk of their own well-informed choices, provided that these choices have not been distorted by obvious fraud and similar defects of consent. An obligation on a payment service provider to refuse to execute potentially detrimental payment transactions, in order to protect the payment service user, seems generally inconsistent with this principle.[84]

4.6 Defining when a PSP took sufficient action to combat fraud

39. In our view, this all leads to the conclusion that the PSP could possibly prove that it acted sufficiently to mitigate the risk that the PSU would fall victim to fraud. This ties into our next section about negligence of the PSU. If the PSP took sufficient action to make the PSU change course in terms of warning and suspending transactions, but the PSU nevertheless persisted in transferring funds to the fraudster, this may lead to the conclusion that PSU needs to bear the loss (partly) himself. As is also the approach in the UK.[85]

---

82 See for example Appellate Body of the Dutch Institute for Financial Disputes 7 February 2025, 2025-0012, https://www.kifid.nl/media/iiihl1mw/uitspraak-2025-0012-pdf.pdf, where the PSP after an internal alert did call the PSU to enquire whether he was a victim of bank impersonation fraud, but the fraudster managed to instruct the PSU to lie to the real bank.

83 See https://www.abc.net.au/news/2024-12-11/singapore-online-scams-bill-restrict-bank-accounts/104693494.

84 Cf. with respect to DCFR information duties: H. Eidenmüller, F. Faust, H.C. Grigoleit, N. Jansen, G. Wagner and R. Zimmermann, 'Der Gemeinsame Refernzrahmen für das Europäische Privatrecht', *Juristenzeitung* 2008, pp. 529-550 (at pp. 544-545).

85 In addition to the mandatory reimbursement requirement in para. 3.2 of Specific Direction 20, the Payment Systems Regulator introduced a number of exceptions from the rule in Part 4 of Specific Requirement 1 (Faster Payments APPP scam reimbursement rules), December 2023 at https://www.psr.org.uk/media/wh5gpfu0/specific-requirement-1-pay-uk-to-amend-fps-rules-dec-2023.pdf. One of these exceptions is the Consumer Standard of Caution in para 4.2. The rules are explained in detail in The Consumer Standard of Caution Exception Guidance, December 2023 at https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf. Under the exception, consumers may be liable to bear the loss if they have 1) disregarded the interventions of the PSP such as warnings; 2) if they have failed to report the fraud to the PSP immediately or within the objective timeframe of 13 months: 3) if they have not cooperated with the PSP on the request for information regarding the payment transaction; 4) and if they have not cooperated with the PSP to report the fraud to the police. These requirements represent the totality of the consumers' standard of care; consumers can be held liable by breaching one or more of the requirements. However, in not showing the required standard of care, consumers have to be grossly negligent. In addition, the Consumer Standard of Caution exception does not apply too vulnerable consumers. The burden of proof is on the PSP to prove the breach. Therefore, according to para. 1.5 of the Guidance '[w]here a PSP can demonstrate that a consumer who has not been classed as vulnerable has, through gross negligence, not met one or more of these four requirements, the PSP is not obliged to reimburse the consumer.'

We also recommend that the EU co-legislator defines what the maximum is PSPs may do (suspending but not blocking and what data can be used with monitoring), because otherwise PSPs themselves will have to walk on this tightrope of monitoring and taking action to manage their liability risk and on the other hand the privacy and autonomy of the PSU.

40. We consider that the PSP should not be able to exonerate himself by proving that no matter how advanced his warning systems, he could not have prevented a scam. There are two main reasons for this. It forces the PSU to debate the inadequacy of the systems of the PSP in court, which a PSU is not equipped to do (see section 3.3 above). It would also lead to the conclusion that precisely the most advanced forms of fraud are for the risk of the PSU. Especially if the PSP could not foresee this fraud scenario, the PSU could not foresee this at all. Liability rules for payment systems should aim for a rational distribution of risk on a systemic level, even if this means that the PSP will sometimes be liable in cases they could not prevent. The current regime for unauthorised transactions applies, even in cases where the PSP could hardly prevent the transaction. Of course, such a risk of liability for (types of) APP fraud is a big step from the current situation of no liability at all for any APP fraud.

5. Gross negligence of the PSU

In the event that the starting point is that the PSP is held liable for (certain types of) APP fraud, it still seems logical that this liability does not apply when the PSU is grossly negligent or acted fraudulently.

5.1 The application of gross negligence may differ per fraud scenario

41. It should be kept in mind that extending liability beyond bank impersonation fraud, even if only in cases that can be traced back to abusing peoples' trust in the financial system, potentially leads to numerous new types of payment fraud covered by the PSR liability regime. As a result, the exception for cases of (fraud or) gross negligence on the part of the PSU will also become more differentiated. A logical but possibly undesirable consequence of expanding liability could be that the exception for gross negligence would be interpreted more broadly as well in practice, with the result that PSUs ultimately have little benefit from it.

In our view, the bar of gross negligence should differ per fraud scenario. For example, a victim of bank impersonation fraud does not have an own interest in believing the fraudster. His intent is good in the sense that he wants to avert risks. However, in some other fraud scenarios, the motivation may be different. For example, in pig butchering scams, the motivation of the PSU is to make financial profit via a really attractive investment opportunity. This is not a motivation you want to stimulate in society, which may suggest that the bar for gross negligence is lower. There the maxim holds "if it is too good to be true, it probably is not true". People should not have an incentive to believe the fraudster, because the upside may be for them whereas the downside is for the PSP. The same would apply for marketplaces scams, where a PSU would be less diligent when ordering goods online when he know he would be compensated.[86] This also ties into our general consideration that

[86] Most credit card companies reimburse a client in case of a scam, but in order for them to be able to do this, they only accept merchants after prior fraud checks and ask these merchants for collateral (normally via the collecting or acquiring PSP).

imposing liability on the PSP in the first place for these cases of fraud is less obvious (see section 4.1).

5.2 Should the application of gross negligence differ per PSU (vulnerable consumers)?

42. One could argue that for vulnerable consumers the bar for gross negligence should be higher. This ties into the special attention devoted in EU consumer law towards vulnerable consumers. Paglietti and Rabitti concluded that the main indicator of vulnerability in case of payment fraud is age.[87] We believe that in the product design level, the age or other aspect of vulnerability of PSUs could indeed play a role. Different consumer groups may need different protection. This aligns with the general idea of product governance, that when designing products or services, the financial institution should ensure that the product is deemed appropriate for the interests, objectives and characteristics of the identified target market(s).[88] On the other hand, we do not believe that vulnerability should play a key role when evaluating gross negligence on behalf of the PSU. The essence is that the mere fact that the PSU became a victim of fraud, shows he is vulnerable for this type of fraud. Also, it would reinforce stereotypes of who is vulnerable. It implies that less is expected from the old or less-educated, which in our view is a signal the co-legislator should not want to give. Ultimately we believe the evaluation of gross negligence should be assessed on a case-by-case basis, taking all the relevant circumstances in account.

5.3 Role of measures taken by the PSP when evaluating gross negligence

43. Moreover, negligence is potentially at play at two moments in the fraud 'journey'. Firstly, at the moment of becoming a target of the fraud. Can the PSU be blamed for not realising he was a target? Preventative measures such as general risk warnings may be relevant here. Also, some PSPs offer creative ways for PSUs to verify whether they are a target of fraud. For example, some PSPs offer a tool in the app to check whether it is indeed the PSP that is calling the PSU. When a PSU did not choose to use this tool and would then fall victim of bank impersonation fraud, this could count towards gross negligence of the PSU. On the other hand, one could doubt whether a PSU at the moment of need can reasonably be expected to use this tool.

Secondly, negligence can also play a role, once the customer was informed by the PSP that he was an actual target of fraud. We believe that if, after a sufficient warning, the PSU nevertheless proceeds with the suspected payment order(s), the liability should flip to the PSU. An alternative view would mean that the PSP cannot manage liability risk, or would have to block transactions even though the PSU knowingly wants to persist in transferring funds to the fraudster. This would be too paternalistic. There have been rare Dutch cases where the court actually ruled that the PSP could have known that the fraudster would target the victim again and therefore should have temporarily blocked the payment

---

87 M.C. Paglietti and M. Rabitti, 'A Matter of Time. Digital- Financial Consumers Vulnerability in the Retail Payments Market', 33, *EBRL*2022(4) pp 602-596.

88 See EBA Guidelines on product oversight and governance arrangements for retail banking products, EBA/GL/2015/18 15 July 2015 guideline 3, https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/consumer-protection/guidelines-product-oversight-and-governance-arrangements-retail-banking-products.

account.[89] We consider this as too paternalistic. See also section 4.6 where we suggest to define when a PSP acted sufficiently to combat APP fraud.

5.4 The duty to cooperate by the PSU to find the fraudster

44. We consider that after having falling victim to fraud, PSUs can be required by their PSPs to cooperate in a reasonable manner. PSPs can require that the victim reports the transaction to the police and assists the PSP in fact finding, helping the PSP to improve his fraud monitoring and if possible recover funds. To a certain extent, this would also protect the PSP against fraudulent claims, as providing false information to the police might be a bridge too far for fraudulent PSUs. For example, if a PSU in the UK does not sufficiently cooperate, this could consequently lead to the conclusion that the PSP will not be held liable.[90]

5.5 Liability cap for PSUs in case of gross negligence?

45. Under the current rules for unauthorised transactions, Member States may cap liability in cases where the PSU is not acting with intent or fraudulently (see section 2.1).[91] Whether this carveout is used will of course influence the assessment of gross negligence under national law; concluding with gross negligence being less dramatic when the financial burden attached is limited.

In PSR, this carveout is maintained for unauthorised transactions.[92] However, in the proposed APP fraud rules in the PSR,[93] no such carveout has been provided. For countries where such carveouts have been made for unauthorised payments, the system will become incoherent if the same liability caps do not apply to the new APP fraud rules. We recommend, therefore, to consider whether a similar Member State's discretion to cap the liability should be included in the proposed APP fraud rules. If not, it would lead to parallel tracks in countries with such a cap. The PSU will likely claim a refund under both provisions, arguing principally on unauthorised payments, which is narrower but the protection is better, and subsidiarily on APP fraud, which is broader but where the protection would seemingly be lower. This might be acceptable, but should at least be discussed.

5.6 Which roles play the EU co-legislator vs the EU member states courts and regulators in defining gross negligence?

46. A difficult question is to what extent the concept of gross negligence should be harmonised in the PSR. Regarding the update of PSD2, the European Banking Authority (EBA) first suggested that the EU co-legislators should clarify the terms 'reasonable grounds

---

89 See Gerechtshof Arnhem-Leeuwarden 24 December 2024, , https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHARL:2024:7950.

90 See section 5.6 below.

91 Article 74 sub 1 and sub 4 Dir. 2015/2366.

92 Article 60 sub 1 and sub 3 PSR.

93 Article 59 PSR.

to suspecting fraud', 'fraudulent act', 'gross negligence' and others.[94] This can be done in multiple ways. Some suggestions we have seen in the negotiations over PSR are:[95]

(i) Giving examples of gross negligence in PSR;

(ii) Giving examples of gross negligence in the recitals to PSR;

(iii) Making EBA responsible to define gross negligence in EBA Guidelines;

(iv) Leaving it entirely to courts and ADR bodies to define gross negligence.

In the Council's Progress Report of 14 June 2024, the Council Working Party does not opt for a definition, but for a 'list of indicative, non-exhaustive criteria' for assessing gross negligence. Given the aim of harmonisation, it is understandable why this is proposed, but we do not really expect the EU co-legislator to be able to predict what kind of fraud consumers will be most vulnerable to in the next 10 years. The advantage of such a list is, of course, that it ensures ample room for a case-by-case assessment by national courts, also taking into account differences in national systems of procedural law. The obvious disadvantage is legal uncertainty. The Report contains three pages with ten detailed non-exhaustive criteria, which could easily be expanded by another ten. Some are very broadly formulated, such as "the payment service user's behaviour or communication with third parties, where relevant". We are quite sceptical towards an enumerating approach in the PSR itself (options (i) and (ii)).

47. In our opinion, such more or less arbitrary criteria provide almost no guidance at all, and carry the risk of gross negligence being too easily assumed. The majority of the authors of this article argue for a definition of "gross negligence" in article 59 of the PSR, possibly combined with some concrete examples of gross negligence in the recitals, showing that this exception to the rule of reimbursement in case of bank impersonation fraud is intended to be a very narrow one. With a view on the Dutch case law, such a definition could be that gross negligence entails a serious degree of culpability on the part of the PSU and that, in order to establish gross negligence, the PSP must prove that the user was aware or should

---

94 Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), EBA/Op/2022/06, 23 June 2022, p. 7 and p. 68, https://www.eba.europa.eu.

95 See Proposal for a Directive of the European Parliament and of 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 and Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 - Progress report, 14 June 2024, 2023/0209(COD), 2023/0210(COD), p. 181, available here. See for the position of the European Parliament Payment services in the internal market and amending Regulation (EU) No 1093/2010 European Parliament legislative resolution of 23 April 2024 on the proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD)) (Ordinary legislative procedure: first reading), 23 April 2024, available here, recital (82) and article 59 sub 5c suggesting that EBA should define gross negligence.

have been aware under the concrete circumstances of a specific risk of becoming victim of payment fraud.[96]

48. What is important here, is that while the private law courts and ADR bodies typically have to define gross negligence in cases for reimbursement between PSPs and PSUs, regulators should in this case also be able to enforce the obligation on PSPs to reimburse their PSUs. For example, if a regulator believes that a PSP too often refuses to compensate due to gross negligence where compensation would be required pursuant to PSR, the regulator may want to fine the PSP. In that sense, the PSR would be quite special, as to our knowledge this would be the first EU regulation where the basis for liability is in the regulation itself and could be enforced by a regulator against a financial institution. For example in MiFID II, IDD and CCD2, there are rules to be met by financial institutions, but in case they are breached these directives do not themselves provide for liability and compensation. Of course, a breach of such a directive is often a tort, breach of contract or unfair commercial practice, but refusing to pay damages is on itself not a breach of regulatory law. We consider that regulators should only impose the rules against PSPs if they have a habit of consistently ignoring jurisprudence of courts or ADR bodies. PSPs may dispute individual cases, but should not have as a strategy refusing to compensate unless a PSU forces the PSP to pay via legal procedures.

6. Others parties in the fraud ecosystem

49. Besides the PSP of the PSU and the involved fraudster, there are also others in the fraud ecosystem, such as the PSP of the payee and electronic communications services providers.

A question is whether the PSP of the payee should also be held liable akin to the PSP of the payer. A fraudster needs a bank account to receive the embezzled funds on.[97,98] The UK has

---

[96] See for example Gerechtshof Den Haag 4 January 2005, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHSGR:2005:AS5273, Rechtbank Amsterdam 14 February 2006https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2006:AV2806, Gerechtshof Arnhem 10 April 2007, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHARN:2007:BA3471 Rechtbank Amsterdam 29 August 2007, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2007:BB3685and more recently Rechtbank Amsterdam29 July 2024, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2024:4973where a preliminary judge in no. 4.4 reconfirms the established burden of proof of the PSP.

[97] A rare exception is when the funds are first send to an account of the PSU itself with a crypto-asset service provider and then the crypto-assets are stolen there. This is rare situation specific for crypto-assets, because other financial assets such as a financial instrument cannot normally be transferred to someone else. See Gerechtshof Arnhem-Leeuwarden 24 December 2024, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHARL:2024:7950 for such a case involving crypto-assets.

[98] Also in Dutch case law there have been successful attempts to hold liable the PSPs of the payee, based on the bank's duty of care (and not PSD2). For example there is a case where Footlocker made a payment to an account that was in the name of Ups, believing they were paying the UPS carrier. Rechtbank Amsterdam 26 July 2017, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2017:5360and Gerechtshof Amsterdam 14 May 2019,https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2019:1611. See for A similar case from Norway is LB-2016-20015 from Borgarting Court of Appeals, where such a claim was considered but did not succeed.

chosen for a split liability between these two PSPs.[99] Within the EU, none of the co-legislators has yet proposed to follow the UK's example. Our view is that such a split liability has as a key advantage that it incentivises the PSP of the payee to combat fraud as well. It also does justice to the fact that both the PSP of the payer and the PSP of the payee profit from offering payment services and should therefore also share in the risks that arise with these services. In the UK this split liability seems to work well, and it even pushed the industry to cooperate.

We believe that, as a general rule, the PSP of the PSU should be the first point of contact for the PSU. Similarly, where a payment initiation service provider (**PISP**) is involved, the PSU can claim with his own PSP who in turn needs to claim with the PISP provided that is where the fault lies.[100] It would be undesirable if PSUs have to reach out to various parties with whom they do not have a relationship and which may be based in other EU Member States.

50. Interestingly, besides PSPs, electronic communications services providers (including social media companies) are legally enlisted in the fight against APP fraud. Where informed by a PSP of the occurrence of this type of APP fraud, electronic communications services providers shall cooperate closely with PSPs and act swiftly to ensure that appropriate organisational and technical measures are in place to safeguard the security and confidentiality of communications, including with regard to calling line identification and electronic mail address.[101] The EP suggest that much more is required from electronic communications services providers, such as educational measures, including alerts to their customers, procedures for reporting fraudulent actions and appropriate organisational and technical measures to safeguard the security of payments users when making transactions. As also indicated in section 3.1 we see merit in this.

7. Recommendations and concluding remarks

Below we list our main recommendations:

51. We believe that the European co-legislator should clarify in PSR: (i) whether a transaction is also authorised if the PSU authenticated this transaction under influence of a fraudster and (ii) to what extent the liability regime under PSD2 leaves room for liability of the PSP based on national private law (for example a PSP's duty of care). The co-legislator should either truly harmonise liability or deliberately leave discretion with Member States. The majority of the authors of this paper are of the view that if the PSU himself initiated and authenticated the transaction even under influence of fraud, this transaction should still be deemed authorised under the PSR.

52. The majority of the authors of this paper are of the view that in PSR, liability for APP fraud should not be limited to cases of bank impersonation fraud, but should also cover other

---

99 See for instance, the UK Payment Systems Regulator's mechanism for APP scams. Specific Requirement 1 (Faster Payment Reimbursement Rule) details the rules on allocating reimbursement between sending and receiving PSPs, splitting the cost of reimbursement 50/50 between the sending and the receiving PSPs and providing rules on communication and cooperation between the PSPs.

100 Article 72 sub 2 and article 90 sub 1 Dir. 2015/2366.

101 Article 59 PSR.

scenarios of payment fraud, provided that peoples' trust in the payment system has been abused by the fraudster (for example police or regulator impersonation). In cases of payment fraud *not* directly associated with peoples' trust in the payment system (for example WhatsApp fraud, invoice fraud or relationship fraud), it should be left at the Member State's discretion whether or not to allocate liability to the PSP (for example based on a PSP's duty of care pursuant to national law).

53. The majority of the authors of this paper argue for a definition of "gross negligence" in the context of APP fraud in the PSR, possibly combined with some concrete examples of gross negligence in the recitals, indicating that this exception to the rule of reimbursement in case of impersonation fraud involving peoples' trust in the payment system is intended to be a very narrow one. Such a definition could be that gross negligence entails a serious degree of culpability on the part of the PSU and that, in order to establish gross negligence, the PSP must prove that the user was aware or should have been aware under the concrete circumstances of a specific risk of becoming victim of payment fraud.

54. The majority of the authors believe that the European co-legislator should specify to what extent PSPs can monitor transactions in order to combat fraud and to what extent PSPs can suspend transactions or apply cooling-off periods for large transactions, especially taking into account the recent Instant Payments Regulation which sets as a rule that transactions need to be instant.

55. In the future, the EU may consider whether consumer protection from third party fraud that can be traced back to abusing peoples' trust in the financial system should move beyond the area of payments. Considering the aim of maintaining trust in the security of financial services, the EU co-legislator may consider expanding consumer protection by allocating liability to the financial institutions in cases of fraudulent misuse of electronic signatures more generally.[102],[103] The rollout of the European Digital Identity Wallet under the revised eIDAS-Regulation makes this even more relevant, as it is suggested that the European Digital Identity Wallet can be used to authorise payment transaction and other financial transactions.[104] The question then, is whether EU law will protect the users of the EDIW only when it is used for payments, or whether victims other fraud cases, such as credit fraud, should be brought under the same protective umbrella.

***

---

102 M. Eidsand Kjørven, 'Who Pays When Things go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe', 31. *EBLR* 2020(1), p 107.

103 For example, in countries where the banking sector is highly digitised and utilises public or *de facto* public electronic identity system, like Scandinavia and Estonia, digitalisation of credit agreements has led to extensive credit fraud. See. extensively , V.Wold and P. Kalamees, 'Identity Theft in Consumer Finance: Consent, Contract and Liability – Analysing Rules on Loss Allocation in Norwegian, Estonian and EU Law', (forthcoming in *Oslo Law review*, 2025).

104 Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, recital (56), https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng.