DOI: 10.14324/111.444.2052-1871.1988

Authorised Push Payment Fraud: Theorising a Loss Allocation Model

Nat Shum[*]

Abstract: Authorised push payment fraud ('APP fraud') occurs when a bank customer authorises the transfer of funds from their accounts, under a false pretence set up by a fraudster. The UK mandatory reimbursement regime and the EU Proposal for the Payment Services Directive 3 present wholly different loss allocation models in response to APP fraud. This article explores the following question: *how should losses be allocated between the customer who authorises the transaction and their financial institution*? The classic experience in formulating loss-allocation rules for *unauthorised* fraud provides a case-in-point as to whether banks should bear the bulk of the losses for APP fraud. By examining the distinction between authorised and unauthorised fraud, this article presents a principled case of a loss-allocation model that reflects the concepts of fault and moral hazard. In summary, this article argues for a loss allocation model that considers customer fault, the absence of a fixed upper limit on customer liability, increased bank liability for banks that their duties, and the exclusion of exceptions for vulnerable customers. The proposed loss allocation model aims to strike a balance between customer protection and financial consequences for banks, advocating for a shared liability approach between customers and banks. Regarding the concepts of fault and moral hazard, this proposed model suggests specific duties for banks to prevent authorised fraud and addresses the issue of moral hazard by incentivizing customers to take reasonable care in identifying fraud patterns. This proposed model serves to provide a starting point for future research and policy development in this area.

Keywords: Authorised Push Payment (APP) fraud, mandatory reimbursement, Payment Services Directive (PSD 2 & PSD 3), loss allocation model, payments, financial regulation.

A. INTRODUCTION

Authorised push payment fraud ('APP fraud') has emerged as a new type of financial fraud, whereby the victim is induced by fraudulent means to authorise their bank to send a payment to a bank account, which is controlled by the fraudster. APP fraud is contrasted against pull payment fraud or unauthorised fraud, where payments are extracted from the victim's bank account or debited to a card by a criminal, without the victim's authority.[1] In 2020, €323 million is the estimated value of total APP fraud losses for all Single Euro Payments Area euro credit transfers in the EU.[2] In 2023, 252,626 APP fraud cases and £341 million in losses were

[*]The author holds an LL.B. degree from University College London and Hong Kong University and PCLL from Hong Kong University. E-mail: natshumyc@gmail.com.

[1] *Philipp v Barclays Bank UK plc* [2023] UKSC 25, [2023] 3 WLR 284, [8].

[2] European Commission, 'Commission Staff Working Document – Impact Assessment Report – Accompanying the documents 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; 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; Directives 2015/2366/EU and 2009/110/EC' SWD/2023/231 final ('EU Impact Assessment Report for PSD 3'), 10.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

reported in the UK.[3] The existence of APP fraud as a social problem has prompted a multitude of solutions by regulators, including the creation of fraud prevention entities, data sharing and collaboration, risk and security, resolution frameworks, and the allocation of liability.[4]

This article focuses on allocation of liability between the customer who authorises the transaction and their financial institution (rather than other stakeholders in fraud prevention policies), primarily because financial institutions play the chief role in safeguarding customers' funds. [5] Frameworks to allocate liability between the customer and their financial institution are proposed by the EU and UK, under the new mandatory reimbursement requirement[6] and Proposal for Payment Services Directive 3 ('PSD 3')[7] respectively. These proposed loss allocation frameworks alter the position that losses lie where they fall 'namely, with customers) for want of regulatory intervention.

The Part 1 shall explore is '*how should losses be allocated between the customer who authorises the transaction and their financial institution?*' The structure of this article is as follows. In Part 2, I present the existing framework and proposals of loss allocation regimes for authorised fraud and unauthorised fraud. I summarise the main legislations provided for loss allocation in unauthorised fraud, namely, the EU Payment Services Directive 2 ('PSD 2'),[8] US Electronic Funds Transfer Act (also known as Regulation E, hereinafter as 'Reg E'),[9] and

[3] Payment Systems Regulator, 'Authorised push payment (APP) scams performance report' (July 2024) <https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/> accessed 22 February 2025.
[4] Lipis Advisors, 'Fraud prevention and resolution in push payment systems – comparative analysis' (*Payment Systems Regulator,* 2017) <www.psr.org.uk/media/3dbln5tw/lipis-report-international-fraud-practices-msg_.pdf> accessed 22 February 2025, 13. For a list of industry responses in the UK, ibid 6-7.
[5] In addition to financial institutions, regulators have sought to impose duties on other stakeholders to prevent fraud, for instance, telecommunication companies that have the duty to implement a scam filter: Monetary Authority of Singapore, 'Guidelines on Shared Responsibility Framework' (24 October 2024) <https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/pso/guidelines-on-shared-responsibility-framework/guidelines-on-shared-responsibility-framework.pdf> ('Singapore Guidelines').
[6] Payment Systems Regulator, 'Policy Statement – Fighting authorised push payment fraud: a new reimbursement requirement – Response to September 2022 consultation (CP22/4)' PS23/3 (June 2023) <https://www.psr.org.uk/media/rxtlt2k4/ps23-3-app-fraud-reimbursement-policy-statement-june-2023.pdf> accessed 22 February 2025 ('UK Jun 2023 Policy Statement'); Payment Systems Regulator, 'Policy Statement – Fighting authorised push payment scams: final decision' PS23/4 (December 2023) <https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf> accessed 22 February 2025 ('UK Dec 2023 Policy Statement').
[7] European Commission, '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' COM/2023/366 final (EU Proposal for PSD 3); European Commission, '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/2023/367 final ('EU Proposed Payment Services Regulation').
[8] Council Directive 2015/2366/EC of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35 ('PSD 2').
[9] 15 U.S.C. 1693 (1978).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

US Uniform Commercial Code ('UCC') Article 4A.[10] These loss allocation regimes prescribe duties borne by financial institutions and customers when dealing with unauthorised fraud, and provide the situations when (and the extent to which) they respectively bear fraud losses (Sections 2.1 and 2.2). I will then review the UK and EU proposals that mirror, to different extents, the legislation on unauthorised fraud which provides compensation to customers (Section 2.3).

In Part 3, I theorise a loss allocation model for authorised fraud that reflects its theoretical and policy considerations, by exploring (i) the comparative lens of the regulatory responses to unauthorised fraud, and (ii) the theoretical lens of customer protection and moral hazard. I shall make four conclusions on the loss allocation model: (i) the loss allocation model should reflect customer fault in authorised fraud (Section 3.1); (ii) there should not be a fixed upper limit of customer liability (Section 3.2); (iii) the extent of liability of banks should reflect whether the bank is at fault (Section 3.3); and (iv) vulnerable customers do not warrant a separate set of loss allocation rules (Section 3.4). The theorised model based on these four principles thus form an indirect critique of the UK and EU proposals.

B. Distinction Between Authorised and Unauthorised Fraud

1. Unauthorised fraud by design

As PSD 2, Reg E, and UCC Article 4A show, regulatory responses to fraud have historically focused on unauthorised fraud.

(i) EU PSD 2

PSD 2 Articles 66-77[11] govern unauthorised fraud and loss allocation. The key underpinning is that a payment transaction binds a payment service user ('user') only when he authorises the payment, namely, where the payer's consent to execute the payment transaction[12] in the form[13] and procedure[14] is agreed between the payer and the payment service provider ('PSP'). In the absence of such consent, a payment transaction is unauthorised.

[10] Uniform Commercial Code, Article 4A.
[11] For a general overview of these provisions, see Gabriella Gimigliano, 'Authorisation of Payment Transactions (Arts 64–77)' in Gabriella Gimigliano and others (eds), *The Payment Services Directive II - A Commentary* (Edward Elgar, 2021).
[12] Payment Services Directive 2, Art. 64.
[13] Payment Services Directive 2, Art. 64(2).
[14] Payment Services Directive 2, Art. 64(4). It follows that an agent with actual authority may fail to authorise if the user has not informed the PSP of the agent's status.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

The verification of authorisation by means of a payment instrument – in other words, authentication – may be proof of authorisation.[15]

Where a transaction is unauthorised:

i. The starting point is that the PSP bears the loss of the fraud amount, only if the user notifies the PSP promptly of the loss.[16] In this case, the PSP must refund the user immediately for the amount of unauthorised transactions. If the user fails to fulfil the notification requirements, the user bears the loss.

ii. However, the user shall bear all losses if they act fraudulently, or fail to fulfil one or more of the obligations set out in Art. 69[17] with intent or gross negligence.[18] Gross negligence means "conduct exhibiting a significant degree of carelessness", and includes "keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties".[19] Under Art. 69,[20] the duties of the user[21] include, *inter alia*, the duty to "take all reasonable steps to keep safe the personalised security payment instrument".[22]

iii. In other circumstances, such as when the user does not breach the duty under Art. 69,[23] or breaches the duty under Art. 69 but was neither intentional nor grossly negligent,[24] the user may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50. This results from the use of a lost or stolen payment instrument or the misappropriation of a payment instrument.[25]

[15] Payment Services Directive 2, Art. 72.
[16] Without undue delay on becoming aware of any such transaction giving rise to a claim and no later than 13 months after the debit date: PSD 2, Art. 71(1).
[17] Payment Services Directive 2, Art. 69.
[18] Gross negligence may include cases that would have otherwise been treated as those of apparent authority, for example, cases of familiar fraud where the payment service user delivers the payment instrument to a person considered by the payment service user to be a trusted agent who nevertheless betrays them: Benjamin Geva, 'Electronic Payments: Guide on Legal and Regulatory Reforms and Best Practices for Developing Countries' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3631155> accessed 22 February 2025, 58.
[19] Payment Services Directive 2, Preamble (72).
[20] Payment Services Directive 2, Art. 69.
[21] Art. 69 imposes a broad duty to "use the payment instrument in accordance with the terms governing the issue and use of the payment instrument".
[22] Further, Payment Services Directive 2, Art. 74 expressly provides a number of situations where that the PSP shall bear the entire loss when the payer has not acted fraudulently, including where (i) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, (ii) where the loss is caused by acts or omissions by the PSP, (iii) the payer's PSP does not require 'strong customer authentication', (iv) further theft or misappropriation of the payment instrument or its unauthorised use after prompt notification, and (v) where the PSP does not provide appropriate means for the notification.
[23] Payment Services Directive 2, Art. 69.
[24] Geva, 'Guide on Legal and Regulatory Reforms and Best Practices for Developing Countries' (n 16), 59.
[25] Payment Services Directive 2, Art. 74(1).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

Authentication does not lead to a presumption, conclusive or otherwise, that the payment is authorised under Art. 64.[26] In other words, it remains open for the user to challenge the authorisation, notwithstanding compliance with the form and procedure of giving consent as agreed by the user and the PSP. Where the user denies having authorised a payment transaction as debited to their account, it remains with the PSP to furnish additional proof to show that the transaction was authorised. This rule, as newly introduced in PSD 2 in 2015, is explained by reference to the customer's limited opportunity to provide evidence in cases of online payment fraud.[27] By the' same token, the fact that there is proper authorisation means that the user is bound by the transaction. PSD 2 could thus be seen to protect the sanctity of authorisation, in light of how, under the irrevocability of a payment order, a user must not revoke a payment order once it has been received by the payer's PSP.[28] To that extent, it informs us how regulatory responses to authorised fraud shall have regard to the centrality of the authority concept.

(ii) US Regulation E

In the US, unauthorised consumer transfers and non-consumer transactions are governed separately. Reg E[29] governs unauthorised consumer transfers. The underlying principle is that a consumer is liable for authorised transfers,[30] until the time of notification to the bank.

The loss allocation rules under Reg E §205.6.73[31] for unauthorised consumer transfers are as follows[32]:

i. If the consumer notifies the financial institution within two business days, after learning of the loss or theft of the access device, the consumer's liability is at most $50.[33]

[26] This is because the use of a payment instrument recorded by the [PSP] shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Art. 69: Payment Services Directive 2, Art. 72.
[27] Payment Services Directive 2, Preamble (72); Marte Eidsand Kjørven, 'Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe' (2020) 31(1) EBLR 77-109, 89-90.
[28] Payment Services Directive 2, Art. 80.
[29] Reg E
[30] Namely, electronic fund transfers that fall outside of the definition of "unauthorised electronic fund transfers" under Reg E §205.2(m).
[31] Reg E §205.6.73.
[32] For a general overview of rules governing unauthorised *consumer* transfers under Reg E, see Benjamin Geva, *Bank Collections and Payment Transactions: A Comparative Legal Analysis* (OUP, 2001) 410-413.
[33] Reg E §205.6(b)(1).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

ii. If the consumer fails to notify the financial institution, within two business days after learning of the loss or theft of the access device, the consumer's liability is at most $500.[34]

iii. A consumer must report an unauthorised electronic fund transfer that appears on a periodic statement within 60 days of the financial institution's transmittal of the statement to avoid liability for subsequent transfers. If the consumer fails to do so, the consumer may bear the loss for the entirety of the unauthorised transfers that occur after the close of the 60 days and before notice to the institution.[35]

These provisions provide the consumer with the duty to notify the financial institution of the loss or theft of the access device or of an unauthorised transfer that appears on a periodic statement. Crucially, only electronic fund transfers executed with fraudulent intent by the consumer (or any person acting in concert with the consumer) are deemed to be authorised by the consumer, and binds the consumer.[36]

(iii) UCC Article 4A

The rules under UCC Article 4A governing unauthorised non-consumer[37] transfers are as follows:[38]

i. The starting point is that the customer is liable for anything which binds them under agency,[39] be it express, implied or apparent authority.[40]

ii. Additionally, the customer bears the loss for *unauthorised* payment orders, accepted by the bank in good faith, whereby the authenticity was verified by the bank pursuant to a commercially reasonable security procedure which was agreed between the customer and bank.[41] Where payment transactions are not authenticated by the prescribed methods, the bank bears the loss and must refund the customer the amount of the unauthenticated payment order, even when the customer fails to notify the bank of the unauthorised payment within a reasonable time (not exceeding 90 days).[42]

[34] Reg E §205.6(b)(2).
[35] Reg E §205.6(b)(3).
[36] Reg E §205.2(m).
[37] UCC §4A-108.
[38] For a general overview of rules governing unauthorised *non-consumer* transfers under UCC Article 4A, see Geva (n 26) 405-410.
[39] UCC §4A-202(a).
[40] Geva, Bank Collections and Payment Transactions (n 26), 406 [16].
[41] UCC §4A-202(b).
[42] UCC §4A-204(a).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

iii. However, for authenticated transactions, the bank bears the loss where the customer proves that the order was caused by an interloper, namely, an outsider to the customer's organisation.[43]

In the case of non-consumers, a payment instruction that is purportedly authorised by the customer binds the customer. It only matters that the payment instruction emanates from the customer, such as when an insider of the customer – without actual or apparent authority – successfully uses the agreed security procedure to execute the transaction, even where the insider is not proximate to the transmitting facilities and the access.[44] This may be justified on the basis that the bank should be allowed to assume that matters of the customer's internal management and procedure have duly been complied with.[45]

2. The Authorised-Unauthorised Distinction

(i) Typologies of authorised fraud under the three regimes

With reference to the common law concept of authority, conclusions can be drawn for a few categories of cases:

i. For transactions executed by a principal themselves, or an agent with actual authority to do so, they are treated as authorised under all three regimes.[46] This is consistent with common law agency principles, under which, an act binds a principal where it is done by (i) themselves or (ii) an agent with actual authority, someone to whom the principal, expressly or impliedly, directs to act on their behalf.[47]

ii. For transactions executed by an agent with apparent authority, they are treated as unauthorised under PSD 2[48] and Reg E[49] (subject to the situation of familiar fraud under the third conclusion below). For instance, under PSD 2, methods to issue a payment instruction must abide by the agreed-upon procedure to constitute proper authentication.[50] This prevents the PSP from claiming that the user has, by some means otherwise, represented that the agent is authorised. Thus, PSD 2 eliminates the

[43] UCC §4A-203(a)(2).
[44] Geva, Bank Collections and Payment Transactions (n 26), 408 [17].
[45] Resembling, but going even further than, the Turquand's rule or indoor management rule under common law: *Royal British Bank v Turquand* [1856] 6 E. & B. 327 (Court of Exchequer); *Mahony v East Holyford Mining Co* (1874-75) LR 7 HL 869, 894.
[46] See Payment Services Directive 2, Art. 64, Reg E §205.2(m), and UCC §4A-202(a). These three frameworks do not modify the common law position of actual authority.
[47] Peter George Watts and Francis Reynolds, *Bowstead & Reynolds on Agency* (23rd edn, Sweet and Maxwell 2023) 3-003.
[48] Payment Services Directive 2, Art. 64.
[49] Reg E, §205.2(m).
[50] Payment Services Directive 2, Art. 64.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

possibility of apparent authority.[51] This is slightly different from the common law position, whereby a principal is bound against the third party to whom the agent acts with apparent authority, which arises when (i) the principal (or someone with actual authority on their behalf) represents to the third party that the agent has such authority, and (ii) the third party is induced by and relies on the representation.[52]

iii. For transactions executed by an agent to whom the customer gives the access device, they may be treated as authorised under Reg E[53] and PSD 2.[54] Under Reg E, transactions by an agent who was furnished the access device to the consumer's account by the consumer – with apparent authority since the consumer has once notified the financial institution that transfers by the agent are authorised – are expressly deemed to be authorised, and so binds the consumer.[55] This is so, notwithstanding the agent may have acted beyond the scope of their actual authority (e.g. stole funds from the principal). By contrast, the situation is less clear under PSD 2. The situation of an agent who has transgressed the scope of their actual authority – but with apparent authority – warrants more consideration as they may well have passed the proper authentication procedure. That said, the principal may have breached the obligation to "keep personalised security credentials safe" under Art. 69[56] with intent, thus, rendering the transaction binding on the principal.[57] Conversely, it may be that the principal could adduce evidence that the agent is not authorised to rebut the finding of authorisation under Art. 64 PSD 2,[58] such that the transaction does not bind them. Due to ambiguity under PSD 2, familiar fraud should generally be seen to be an instance of authorised fraud, which must be accounted for in the loss allocation model. However, this situation of familiar fraud falls within apparent authority under common law and binds the customer.

iv. Fourth, a transaction executed by a person with neither actual nor apparent authority is firmly unauthorised under all three regimes. This follows from the trite principle that an agent may not clothe themselves with actual or apparent authority

[51] Geva, Bank Collections and Payment Transactions (n 26), 55.
[52] ibid 3-004; *Freeman & Lockyer v Buckhurst Park Properties Ltd* [1964] 2 QB 480 (CA).
[53] Reg E §205.2(m).
[54] Payment Services Directive 2, Arts. 64 and 69.
[55] Unless the consumer has notified the financial institution that transfers by that person are no longer authorised: Reg E §205.2(m).
[56] Payment Services Directive 2, Art. 69.
[57] Marte Eidsand Kjørven (n 23), 88; Payment Services Directive 2, Art. 69(2).
[58] Payment Services Directive 2, Art. 64.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

simply by saying so.[59] Under apparent authority, any representation must originate from the principal, and not the agent. As such, a rogue who has gained access to a security device is not authorised within category (3) above. This category may apply for phishing and spoofing fraud where the payer voluntarily sends their personal credentials/ verification code to others (and acts with pre-fraud fault), or for hacking, identity theft, or malware-enabled variants fraud[60] (where the payer is innocent).

(ii) What does 'authorised fraud' mean?

In all cases of authorised fraud, it is the customer, rather than the fraudster, [61] who executes the payment instructions. Authorised fraud includes two major categories of APP fraud: [62]

i. Malicious Redirection Fraud: This refers to a situation where the customer thinks, in good faith, that they are sending money to the payee, where they are sending money to a fraudster. This includes invoice fraud, CEO fraud, impersonation by police or bank staff and other forms of impersonation.

ii. Malicious Payee Fraud: This include investment scams, romance scams, purchase scams, and advance fee scams. It refers to the situation where the payer fully intends to send the payment to a fraudster and thus authorises the payment, but is defrauded under the pretence set up by the fraudster.

Two observations may be made concerning the nomenclature of authorised fraud. First, situations that straddle the fine line between unauthorised and authorised fraud exist. An example is familiar fraud following the analysis on principle (3) in Section 2.2.1. Another example could be a mixed social engineering and technical fraud, where the customer hands over personal security credentials to the fraudsters, and it is the fraudster who authenticates the

[59] *Armagas Ltd v Mundogas SA (The Ocean Frost)* [1986] AC 717 (HL).
[60] Monetary Authority of Singapore, 'Consultation Paper on Proposed Shared Responsibility Framework' P016-2023 (October 2023) <www.mas.gov.sg/publications/consultations/2023/consultation-paper-on-proposed-shared-responsibility-framework> accessed 22 February 2025, [4.4].
[61] For instance, where the customer hands over their personal credentials/ SMS verification code to the fraudster, e.g. by clicking on a phishing link and entering their credentials on a fake digital platform, and the fraudster executes the payment instruction: Singapore Consultation Paper (n 48), [4.1]; or where the customer enrols the fraudster's devices as a factor of the strong customer authentication (***SCA***) system, allowing the fraudster to take over the payment account completely: European Banking Authority, 'Opinion on new types of payment fraud and possible mitigations' EBA-Op/2024/01 (29 April 2024) <www.eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf> accessed 22 February 2025 (EBA Opinion), [23].
[62] UK Finance, 'Half Year Fraud Update 2023' (*UK Finance,* 24 October 2023) <www.ukfinance.org.uk/system/files/2023-10/Half%20year%20fraud%20update%202023.pdf> accessed 22 February 2025, 27.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

payment. While such cases are technically unauthorised, the latest opinion of the European Banking Authority ('EBA') observed that PSPs often wrongly categorise such fraud as authorised.[63]

Regardless of the precise categorisation, since the UK and EU expressly only aim to tackle APP fraud rather than authorised fraud generally, [64] this article principally takes the same approach in devising the loss allocation model. Future proposals should clarify whether familiar fraud falls within the scope of either or neither of the regimes for unauthorised and authorised fraud.[65] Second, in any event, regulatory intervention must account for the ever-evolving typologies of authorised fraud, due to its broad catch of all types of payment frauds notwithstanding unauthorised fraud and changing fraud technologies. On one hand, the loss allocation rules must be flexible enough to meet the changing specific nature of each type of authorised fraud and account for specific and nuanced responses. On the other hand, since authority is the unifying factor, there must be clear principles unifying the allocation rules for different types of authorised fraud. As we shall see in Section 3.3, the duty-based view on banks resolves this apparent conflict.

3. Existing Proposals for Authorised Fraud

(i) The UK's mandatory reimbursement requirement

In June 2023, the UK's Payment Systems Regulator ('PSR') confirmed new mandatory reimbursement requirements (hereinafter, 'the UK regime') for APP fraud within the Faster Payments System.[66] It reforms the current Contingent Reimbursement Model Code[67] ('CRM Code') that came into effect in May 2019. In December 2023, the PSR introduced the final detailed parameters and legal instruments to implement the mandatory reimbursement requirement, including the maximum level of reimbursement, claim excess, and the applicable

[63] EBA Opinion (n 49), [23].
[64] See, for example, how the UK and EU policy papers proceed on the basis of APP fraud *alone*: Payment Systems Regulator, 'Report and Consultation – Authorised push payment scams: PSR-led work to mitigate the impact of scams, including a consultation on a contingent reimbursement model' CP17/2 (November 2017) <https://www.psr.org.uk/media/1scay2wu/psr-app-scams-report-consultation.pdf> accessed 22 February 2025; EU Proposal for PSD 3 (n 7), 5.
[65] Along these lines, the EBA has observed the need to clarify certain fraud typologies that are easily mistaken as authorised as unauthorised fraud. Crucially, the EBA's classification of authorised and unauthorised fraud also proceeds on the concept of authority as adopted in this article, to ask whether it is the *customer* who gives the payment order: EBA Opinion (n 49), [31(a)].
[66] UK Jun 2023 Policy Statement (n 6).
[67] Lending Services Board, 'Contingent Reimbursement Model Code for Authorised Push Payment Scams (17 October 2023)' <www.lendingstandardsboard.org.uk/wp-content/uploads/2023/10/LSB-CRM-Code-V5.0-17-October-2023.pdf> accessed 22 February 2025 (***CRM Code***).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

consumer standard of caution.[68] The UK regime came into effect on 7 October 2024.[69] Under the UK regime, PSPs shall reimburse in-scope customers who fall victim to APP fraud in most cases fully for their loss unless customers act fraudulently or with gross negligence,[70] subject to the claim excess of up to £100 per claim from the customer. [71] The receiving PSP and the sending PSP shall apportion the loss on a 50:50 basis. [72] The maximum amount of reimbursement is fixed at £85,000,[73] and customers bear all losses above this level. Sending PSPs must reimburse customers who fall victim to APP fraud within five business days,[74] except where the clock is stopped temporarily to permit the sending to PSP to gather further information.[75] This time limit is shorter than 15 business days, under the CRM Code.[76] Sending PSPs will have the option to deny APP fraud claims which have been submitted more than 13 months after the final payment to the fraudster.

Additional protections are provided for vulnerable customers, [77] namely, that the customer standard of caution and claim excess must not be applied. [78] In other words, notwithstanding their gross negligence, vulnerable customers will be reimbursed in full regardless of the £100 limit.[79] PSPs must consider a range of factors in construing vulnerability and must ask the extent to which characteristics of vulnerability of the customer, whether temporary or enduring, led them to be defrauded.[80]

Customers bear loss when they act fraudulently or with gross negligence. Gross negligence is a "high bar", and the burden of proof is on the PSP.[81] Further, gross negligence is only limited to the failure to fulfil any of these four specific duties: (i) have regard to interventions by the PSP or the police; (ii) promptly notify the matter to their PSP and not more

[68] UK Dec 2023 Policy Statement (n 6).
[69] UK Dec 2023 Policy Statement (n 6), [1.5].
[70] UK Jun 2023 Policy Statement (n 6), p.6.
[71] UK Dec 2023 Policy Statement (n 6), [1.2].
[72] UK Jun 2023 Policy Statement (n 6), [1.3].
[73] Payment Systems Regulator, 'Policy Statement – Faster Payments APP scams reimbursement requirement: Confirming the maximum level of reimbursement' PS24/7 (October 2024) <https://www.psr.org.uk/media/e30pwlly/ps24-7-app-scams-maximum-level-of-reimbursement-policy-statement-oct-2024.pdf> accessed 22 February 2025.
[74] UK Jun 2023 Policy Statement (n 6), [5.18].
[75] ibid [5.22].
[76] R3(1) of the CRM Code (n 55). Note in exceptional cases, this period can be extended to a maximum of 35 business days, provided the firm informs the Customer of the delay and the reasons for it, and the date by which the decision will be made.
[77] A vulnerable customer is defined as "someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care": UK Jun 2023 Policy Statement (n 6), [2.12].
[78] UK Jun 2023 Policy Statement (n 6), [2.11].
[79] UK Jun 2023 Policy Statement (n 6), [1.3].
[80] UK Jun 2023 Policy Statement (n 6), [2.13].
[81] UK Jun 2023 Policy Statement (n 6), ft 8.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

than 13 months after the last relevant payment was authorised; (iii) respond to their PSP's requests for information, and (iv) report the scam to the police.[82] As for duties on PSPs, PSPs shall communicate their assessment of the probability that an intended payment is an APP scam payment.[83] By contrast, gross negligence under R(2)(1)(e) of the CRM Code[84] is not defined. The UK regime thus modifies the scope of gross negligence under the CRM Code.[85]

(ii) EU Proposal for PSD 3

Compared to the UK regime, the EU has taken a much more restrained approach. In its Impact Assessment Report for PSD 3,[86] the Commission rejected the "full reversal of liability between users and PSPs" for authorised fraud.[87] The EU introduces refund rights for authorised fraud (conditional reversal of liability) by the payer's PSP in two narrow situations.[88] First, reimbursement is granted for users (not just consumers) who suffered damages caused by the failure of the International Bank Account Number ('IBAN') / name verification service to detect a mismatch between the name and IBAN of the payee.[89] PSPs must offer the IBAN/name verification service and inform the payer of the degree of match between the name and IBAN of the payee.[90] This allows the payer to decide whether to proceed with the transfer. The PSP(s) (payer and/or payee PSP) that failed to notify the payer of a detected discrepancy between the unique identifier and the name of the payee provided by the payer must refund the payer the full amount.[91] As a matter of authorised fraud, this specifically tackles invoice fraud where the payee's account number but not the name is substituted with the fraudster's, as well as erroneous payment transactions, which are authorised transactions but not fraud.

Second, reimbursement is granted for consumers who fall victim to a specific type of spoofing fraud, namely, where the fraudster impersonates an employee of the consumer's PSP using the bank's name, email address, or phone number.[92] Refund is subject to the consumer filing a police report and notifying their PSP without delay. Refund is not available where the

[82] UK Dec 2023 Policy Statement (n 6), [1.2].
[83] UK Dec 2023 Policy Statement (n 6), [5].
[84] R2(1)(e) of the CRM Code (n 55).
[85] Note that R2(1) of the CRM Code (n 55) provides additional grounds for user liability.
[86] EU Impact Assessment Report for PSD 3 (n 2).
[87] EU Impact Assessment Report for PSD 3 (n 2), [6.1.d].
[88] Note that technical service providers and operators of payment schemes could be liable for the failure to support the application of strong customer authentication: EU Proposed Payment Services Regulation (n 7), Art. 58.
[89] ibid Art. 57.
[90] EU Proposed Payment Services Regulation (n 7), Art. 50.
[91] EU Proposed Payment Services Regulation (n 7), Art. 57(2).
[92] EU Proposed Payment Services Regulation (n 7), Art. 59(1).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

consumer acts with gross negligence or intent,[93] including where they fall victim to the same fraud more than once, or to fraud which is not convincing, such as other than the bank's advertised credentials.[94]

PSD 3 is a restrained response compared to a wholesale reform in the UK case, which tackles all types of APP fraud. Whilst the EU justifies the first situation based on the incentivising effect this has on PSPs to adopt IBAN/name verification service,[95] it offers no justification for the second situation. Whilst this may seem to incentivise PSPs to take measures in educating users on how communications from the PSP will be done (e.g. reminding customers that PSPs will not ask for personal credentials or passwords), it is unreasonable and impractical to expect PSPs to actively police impersonation acts to prevent fraudsters from impersonating them. On that basis, there is no principled distinction between the impersonation of the PSP and of other entities. This measure may even be liable to exploitation by fraudsters, who may shift their tactics to impersonating PSPs in hopes of shifting the cost of fraud entirely to PSPs and getting more proceeds.

C. A Principled Case for the Loss Allocation Model for Authorised Fraud

To summarise, the key points of my proposal may be summarised as follows:

i. First, the starting point for loss allocation should be a rule that 'apportions' liability between the customer and the customer's bank in respective proportions, for instance, a 50:50 split. The precise apportionment shall account for the intricate balancing of customer protection against the financial consequences on banks, which should lie within the discretion of regulators. This apportionment rule does not apply to first-party fraud. Three considerations underlie the apportionment approach. First, customers invariably act with pre-fraud fault, which simply follow from the fact that they have duly authorised the transaction. Therefore, the customer's share of loss should be significant to reflect such fault. To that end, no distinction should be made between different levels of customer fault, such as the gross negligence threshold in the UK regime. Second, the apportionment approach removes moral hazard, as the precautionary measures taken by customers and banks are commensurate with the size of payment transactions. Third, compared to erroneous payment transactions, there is a presumption that the lost funds are irrecoverable from the fraudster and have a lower

[93] EU Proposed Payment Services Regulation (n 7), Art. 59(3).
[94] EU Proposed Payment Services Regulation (n 7), Preamble (82).
[95] EU Impact Assessment Report for PSD 3 (n 2), [6.1.e].

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

likelihood of first-party fraud. On that basis, the apportionment approach ought to be used, and there should not be an upper limit on customer liability.

ii. Second, where customers, save for vulnerable customers, breach post-fraud duties, there is good reason to require them to bear the entire loss. This is so, because post-fraud duties, upon the customer's knowledge of their losses, are reasonable and not onerous.

iii. Third, where the customer's bank breaches the duties owed to its customer, it should be responsible for a larger proportion of the loss, compared to the proportion it bears where it satisfies all duties. This reflects the duties owed by banks under the common law, including the *Quincecare* duty (and the limits thereof). Regulators should set the level of increase in the proportion of liability by considering the extent of customer protection and the financial abilities of banks. For instance, a 70:30 split between banks and customers may be prescribed.

iv. Fourth, no special rules should apply with respect to vulnerable customers. If it is assumed that vulnerable customers are incapable of taking any precautionary measures, this provides more of a reason as to why customers should listen to the bank's assessment of the likelihood that they are defrauded. The failure to have regard to such interventions constituting pre-fraud fault in the sense described in Section 3.1 means that losses should lie on them rather than the banks. Further, imposing an additional proportion of liability or the entire liability under the UK regime fails to incentivise banks to protect such customers, resulting in a moral hazard in the sense described in Section 3.1.2. Such a robust policy of customer protection is unlikely to be feasible in most jurisdictions.

1. The model should reflect customer fault, which follows from their authority

(i) Victims of authorised fraud are invariably at fault

For authorised fraud, it can be questioned as to what the relation is between the customer duty to take reasonable care in precautionary measures and loss allocation. A comparison with the models for unauthorised fraud reveals that the UK regime is unprincipled.

Under the unauthorised fraud models, customers bear both (i) pre-fraud and (ii) post-fraud duties to take reasonable care to prevent losses.

For pre-fraud duties:

i. Under PSD 2, the user has the duty to take all reasonable steps to keep safe the personalised security payment instrument. The user bears the entire loss *only* where

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

duties under Art. 69 are breached with intent or gross negligence.[96] In all other situations, the user bears a maximum loss of EUR 50 (subject to fulfilment of post-fraud duties).[97]

ii. In contrast, Reg E disregards the consumer's possible contribution to the fraud as a reason to fasten liability on them. Regardless of pre-fault fault, the consumer may bear only a maximum loss of $50 where the notification requirement is fulfilled.[98]

iii. Under UCC Article 4A, a fault is not the overarching principle for fastening liability. The customer's liability is different depending on whether it is an insider or an interloper who issues the payment order.[99] The customer's fault may well be the same in both cases.

The pre-fraud duties so conceptualised under Art. 69 PSD 2[100] may be said to resemble a duty of reasonable care, which effectively allows PSPs to raise a defence to a claim for the execution of transactions for want of proper authority. Customer fault, on this basis, simply means a breach of the duty that passes a prescribed threshold which renders it just to impose loss on the customer.

Despite the differences among these three regimes on whether fault is the basis to pin liability on the customer, the situation is far more straightforward for authorised fraud. Strictly speaking, customers could not be said to breach a duty as they are entitled to authorise any transactions as they wish. On this basis, customer fault simply means authorising transactions that carry an outcome that they do not want to bear, even though they are, strictly under the authority and agency principles, bound by it and so bear all ensuing losses. This follows from the position under the common law: where the customer authorises the transaction, "[i]t is not for the bank to concern itself with the wisdom or risks of its customer's payment decisions".[101] To this end, there is no reason why customer fault so conceptualised does not apply to authorised fraud. Customer protection, even if accepted as a valid normative principle, should be restrictively applied.

Fault, so conceptualised is largely disregarded by the UK regime since the only type of pre-fraud fault which leads to customer bearing losses, is whether the customer had regard to proper interventions by PSPs and the police.[102] It follows that, whether the customer has

[96] Payment Services Directive 2, Art. 69.
[97] Payment Services Directive 2, Art. 74(1).
[98] Reg E §205.6(b)(1).
[99] UCC §4A-203(a)(2).
[100] Payment Services Directive 2, Art. 69.
[101] *Philipp v Barclays Bank UK plc* year/?(n 1), [3].
[102] UK Dec 2023 Policy Statement (n 6), [5].

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

contributed to the occurrence of fraud in the first place is irrelevant. The narrow conception of pre-fraud fault under the UK regime appears to be similar in scope to the duty to "take appropriate actions in response to effective warnings given by the firm" under R2(1)(a)(iii) of the CRM Code. This reveals that the additional grounds for pre-fraud fault under R2(1)(a) to (d) of the CRM Code are removed.

One could imagine that the narrow notion of pre-fraud fault under the UK regime is found only in the most extreme of situations, such as that in *Philipp v Barclays Bank,*[103] where the victims ignored repeated interventions by the bank staff and police and insisted upon authorising the payment instruction. This appears to be a rather low standard of customer care that comes close to Reg E's approach[104] to disregard the consumer's pre-fraud fault, namely, ignoring the consumer's possible contribution to the fraud as a reason to fasten liability on them. But the considerations for Reg E[105] should not apply, in any event. This is because, unlike authorised fraud where the customer may or may not have contributed to the fraud in the first place such that it may be just to disregard altogether the customer's negligence in contributing to the fraud as relevant, in virtually all cases of authorised fraud, the customer is at fault and contributes to it. Here, it must be emphasised that customer fault would arise simply by virtue of the customer authorising a transaction with an outcome that they do not desire, and is not fault in the sense of the breach of some duty owed to the bank. Such fault on the customer's part should well have been reflected in the model. Thus, limiting gross negligence to the failure to have regard to interventions under the UK regime is problematic.

This problem is even more starkly observed when we compare that with gross negligence under PSD 2.[106] As gross negligence is not further defined under PSD 2,[107] such ambiguity may be said to give more room for the PSPs to interpret gross negligence broadly to reject compensation. It should not be the case that authorised fraud victims, who are always at fault, are more readily compensated for their losses. For unauthorised fraud, it could well be that the customer has done all that he can to prevent losses. Thus, by asking if negligence is gross, it may be distinguished between whether the customer bears all losses, or only up to the prescribed upper limit of customer liability. For authorised fraud, there is little room for the level of fault in this sense to supply a sound basis for just compensation, as customer fault invariably contributes to the fraud. Nor is it easy to discern a principle for just compensation

[103] *Philipp v Barclays Bank UK plc* (n 1).
[104] Reg E §205.6(b)(1).
[105] Reg E §205.6(b)(1).
[106] Payment Services Directive 2, Art. 69.
[107] Payment Services Directive 2, Art. 69.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

based on the typologies of authorised fraud (as explained in Section 2.2.2) and their respective victim profiles.

(ii) Moral hazard should be avoided

It is central to the design of payment rules that both the bank and the customer have enough incentives to pass a certain threshold to take the requisite precautionary measures. Moral hazard are ensued when customers are not incentivised to take precautionary measures for authorised fraud and may take unnecessary risks in relation to payment transactions. More specifically, two types of moral hazard may emerge.

First, a customer who bears no losses has no incentive to take any precautionary measures to prevent fraud. This is the most straightforward conceptualisation of moral hazard. The EU Impact Assessment Report for PSD 3[108] appears to proceed on this view of moral hazard, given that it rejects a full reversal of liability between users and PSPs on the basis that it "only [serves] to reattribute the social cost of fraud *without* incentivising payers to avoid taking unnecessary risks". As considered by Douglass,[109] the zero-liability policy by Visa and Mastercard[110] – where cardholders do not have to bear *any* losses for unauthorised transactions given that they give prompt notification of the loss of the payment card – creates a moral hazard in this sense.[111] In the context of unauthorised fraud, Levitin also considered that this view of moral hazard may go further to allow instances of first-party fraud,[112] namely, that the customer shall falsely allege that a transaction is unauthorised to seek compensation from the bank. Under the UK regime, since a claim excess of £100 may be applied by the PSPs, this view of moral hazard does not arise.

The second type of moral hazard is that a customer who bears *some* losses shall take precautionary measures to prevent fraud, only if the loss that they may bear is greater than the cost of taking additional precautionary measures and/or the benefits received with expediting payment transactions. Where the risk of loss is insufficient to motivate the party to undertake precautionary measures to prevent fraud, the customer would rather bear the loss since it is cheaper to do so. In this light, for the threat of the $50 or $500 loss under Reg E[113] to be

[108] EU Impact Assessment Report for PSD 3 (n 2), [6.1.d].
[109] Duncan B. Douglass, 'An Examination of the Fraud Liability Shift in Consumer Card-Based Payment Systems' (2009) Economic Perspectives Vol. 33, No. 1 <https://ssrn.com/abstract=1341696> accessed 22 February 2025.
[110] See, for example, Visa USA, 'Visa's Zero Liability Policy' <https://usa.visa.com/pay-with-visa/visa-chip-technology-consumers/zero-liability-policy.html> accessed 22 February 2025.
[111] Douglass (n 89), 46.
[112] Adam J. Levitin, 'Private Disordering - Payment Card Fraud Liability Rules' (2010) 5 Brook J Corp Fin & Com L 1, 39.
[113] Reg E §205.6(b).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

effective in incentivising customers to take reasonable care, this threshold must be greater than the cost of precautionary measures and the benefits from *not* taking reasonable care. Similarly, this should also be the case under the UK regime, where customers bear at most £100 liability[114] and are shielded from most of the liability (subject to post-fraud duties).

A few points emerge from this. First, under both Reg E[115] and the UK regime, the threat of customers bearing the entire loss is limited, which may contribute to the rise of moral hazard. This is so since pre-fraud fault is wholly disregarded under Reg E[116] and narrowly construed as only the failure to have regard to interventions under the UK regime,[117] under which, no pre-fraud customer fault can be found if the PSP does not detect the fraud. Contrast this against PSD 2[118] and PSD 3,[119] a threat of fault constituting gross negligence – a concept which is liable to be broadly defined by PSPs under PSD 2[120] and confirmed to be easily found under PSD 3[121] – has a much better bite to incentivise customers to take reasonable care. This reveals how the narrow concept of fault under the UK regime is problematic, and there is good reason for a much broader concept of fault to apply. On the other hand, interpreting the moral hazard problem too literally fails to produce any useful change to the default position of customers bearing the loss. What this foregoing analysis therefore shows, is that customer liability should not be capped as the UK regime does. Rather, customers should bear a significant proportion of their losses.

Second, if this view of moral hazard were tolerated in the eventual loss allocation regime, it could well be that the overall social cost of fraud may increase. A customer may expedite authorisation processes for instructions below a certain amount since the potential loss it bears in relation to fraud is smaller than the costs associated with assuring all transactions are based on a legitimate premise. This concept of moral hazard equally applies to banks, where they may not set up transaction monitoring devices for transactions below a certain amount, since it may be cheaper to compensate the payer than to monitor every payment instruction. Whilst there is nothing that strictly prevents either the party or the bank from preferring to bear

[114] UK Dec 2023 Policy Statement (n 6), [1.2].
[115] Reg E §205.2(m).
[116] Under Reg E §205.2(m), fault on the consumer is relevant only to the extent that electronic fund transfers with "fraudulent intent by the consumer or any person acting in concert with the consumer" are deemed to be authorised.
[117] UK Dec 2023 Policy Statement (n 6), [1.2].
[118] Following how 'gross negligence' is not further defined under PSD 2.
[119] EU Proposed Payment Services Regulation (n 7), Preamble (82).
[120] Following how 'gross negligence' is not further defined under PSD 2.
[121] EU Proposed Payment Services Regulation (n 7), Preamble (82).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

the loss as a matter of *their own* commercial interests, the fact that the rest of the loss is incurred by the other party calls for the need to resolve this aspect of moral hazard.

Third, the query persists as to whether empirical evidence exists to inform the applicable threshold to remove such moral hazard since it requires an express weighing of the costs and benefits of fraud for each party. Particularly, the financial capabilities of individual customers to bear loss differ from customer to customer, and richer customers are more likely to prefer bearing the loss. In these circumstances, no uniform threshold of loss constituting sufficient incentives could be set in principle. As further elaborated in Section 3.2, the difficulty of fixing a standard monetary amount also informs how we should allocate losses based on fixing the *proportion* of the losses instead, e.g. a 50:50 split.

(iii) Post-fraud duties should not be less onerous than unauthorised fraud

As for post-fraud duties, the UK regime provides requirements to notify the PSP and file a police report, where the failure to notify the PSP of the unauthorised transaction within the prescribed time limit of knowing the same results in the customer bearing the entirety of the loss.[122] These duties are reasonable to impose upon the customer's knowledge of their losses, and similar to those under PSD 2[123] and Reg E, [124] where the breach of notification duty within the prescribed time limit results in the customer bearing the *entirety* of the loss. By the same token, for authorised fraud, it is not unreasonable to pin the entire loss on the customer if they fail to satisfy these post-fraud duties.

(iv) The existing models for erroneous transactions provide a case for comparison

The UK regime also departs from the principle taken for erroneous payment instructions – a type of authorised transaction – that losses are shifted to the PSP only if there is fault on the PSP's part. The starting point for these transactions is that the customer bears the loss.[125] For erroneous payment instructions, fault found liability on the bank. Under PSD 3, the PSPs must notify the user of the degree of discrepancy between the name and the bank account number by way of a name-checking service.[126] If the name-checking service fails to

[122] Under the UK regime, the post-fraud duties are the prompt notification, responding to requests for information, and police reporting requirements: UK Dec 2023 Policy Statement (n 6), [5]; cf the post-fraud customer duty not to act "dishonestly or obstructively in a material respect" under R2(2)(b) of the CRM Code (n 55).
As for PSD 3, refund for impersonation fraud is subject to the consumer filing a police report and notifying their PSP without delay: EU Proposed Payment Services Regulation (n 7), Art. 59(1).
[123] Without undue delay on becoming aware of any such transaction giving rise to a claim and no later than 13 months after the debit date: Payment Services Directive 2, Art. 71(1).
[124] Within 60 days of the financial institution's transmittal of the statement: Reg E §205.6(b)(3).
[125] Payment Services Directive 2, Art. 88(1) and (2), UCC §§4A-205 and 206.
[126] EU Impact Assessment Report for PSD 3 (n 2), [6.1.c].

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

detect a mismatch, the PSP bears the loss.[127] Under UCC §§4A-205 and 206, a sender can shift the loss to their bank, only when the receiving bank [128] has failed to comply with an agreed-upon security procedure which would have detected the error.[129] As such, UCC Article 4A[130] and PSD 3[131] provide only limited circumstances where losses for an authorised transaction are recoverable from the bank. As such, they reflect the centrality of the concept of authority – risk for a payment order duly authorised by a payer lies with the payer and is consistent with this concept.

The framework for erroneous payment instructions is a useful comparator for what regulatory responses for authorised fraud should be. As with authorised fraud, the customer is the one at fault – authorising transactions that carry an undesirable outcome. Given that erroneous payment instructions and authorised fraud are, by their very nature, authorised transactions duly executed by the payer on their own volition, the bank – save for their limited duties – has no duty and business to advise the customer on transactions stemming from their proper authority. Here, the fact that the banks can better absorb losses does not provide a reason for adopting an expansive approach imposing bank liability as a starting point.

However, the case of erroneous payment instructions also supplies arguments on why changes should be made to a fault-based approach to reflect the differences between erroneous payment instructions and authorised fraud. First, the framework of rules for authorised fraud should proceed on the basis that the fraudster has absconded with the funds, which may lend some support to the deep pockets argument for banks to bear losses. This is different from erroneous payment instructions, where *realistically*, losses are much more likely to be recoverable from the erroneous payee under restitution and mistake.

Second, authorised fraud sees a much lesser risk of first-party fraud. For erroneous payment instructions, instances of first-party fraud may arise. Customers may abuse the compensation regime by falsely claiming that their transaction is an erroneous one, notwithstanding that they have only later come to regret a payment order and claim that the payment is of a larger sum, or wrongly sent to a payee other than what they truly intended. In such cases, there is a real risk of first-party fraud as the bank has virtually no contrary proof to defeat the customer's factual allegations. However, for authorised fraud, proper rules can

[127] Cf Payment Services Directive 2, Art. 88(5).
[128] UCC §4A-103.
[129] Except when the customer fails to report the error "within a reasonable time, not exceeding 90 days" of being advised of the unauthorised contents: UCC §4A-205(b).
[130] UCC §§4A-205 and 206.
[131] EU Impact Assessment Report for PSD 3 (n 2), [6.1.c].

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

prevent first-party fraud, where the customer so falsely claims authorised fraud in hopes of recouping losses owing to their erroneous instruction. For instance, under the UK regime, the PSP is entitled to request further information from the customer and require the customer to report the matter to the police pursuant to the requirements for a claim for reimbursement.[132] As most instances of first-party fraud may be removed, it is not unfair for banks to bear the loss for authorised fraud.

2. The model should not apply a fixed upper limit of customer liability

(i) The flat excess approach results in the bank bearing the bulk of the losses

Contrasted against the 'all or nothing' approach that imposes the entire loss on one party, in some situations, PSD 2[133] and Reg E[134] adopt the 'flat excess' approach. These provisions provide, subject to a fixed upper limit for customer liability, the PSP or financial institution bears the rest of the losses. Since the prescribed upper limits are not high, one can assume that the PSP or financial institution bears the bulk of the losses. By contrast, the approach under UCC Article 4A is strictly all-or-nothing, where in *all* circumstances, *either* the bank *or* the customer bears the entire loss.[135] The lack of loss-sharing provisions under UCC Article 4A reflects authority as a central construct of the model, under which, the transaction either binds the customer or it does not.

The upper limits under PSD 2[136] and Reg E[137] appear to be arbitrarily determined as the legislators have proffered no empirical evidence on how the figures came to be. The fact that this customer liability – however small in sum – may apply in both cases where the customer has *no* fault at all further speaks volumes to how the flat-excess is not based on sound principle. Rather, it is a symbolic exercise that *formally* shares losses between the customer and the bank. The UK regime, not inconsistent with these observations, entitles the PSP to apply for a claim excess of up to £100 from the customer (except for vulnerable customers).[138]

But even if we accept the arbitrariness of the figure of the flat excess, the justifications for the flat-excess approach under PSD 2[139] and Reg E[140] simply do not apply for authorised fraud since, as argued in Section 3.1, the customer fault level is much higher than that under

[132] UK Dec 2023 Policy Statement (n 6), [5].
[133] Payment Services Directive 2, Art. 74(1).
[134] Reg E §205.6(b).
[135] Section 2.1.3.
[136] Payment Services Directive 2, Art. 74(1).
[137] Reg E §205.6(b).
[138] UK Dec 2023 Policy Statement (n 6), [1.2].
[139] Payment Services Directive 2, Art. 74(1).
[140] Reg E §205.6(b).

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

unauthorised fraud. Particularly, for authorised fraud, it is difficult to merely consider the victims' compliance with the reporting duty without having regard to pre-fraud fault (Reg E) or to speak of their fault level as falling below gross negligence (PSD 2).

(ii) The flat excess approach leads to moral hazard

More fundamentally, the flat excess approach reveals a third aspect of moral hazard (in addition to the two aspects in Section 3.1.2). It applies to a customer who bears *some* losses and is incentivised to take precautionary measures (i.e. the cost of taking additional precautionary measures and/or the benefits received with expediting payment transactions is cheaper than the loss that they may bear). For these customers, as described by Cooter and Rubin, [141] if such incentive is not commensurate with the level of risk of the payment instruction, there is "a point at which liability ceases to produce major increases in loss avoidance behaviour",[142] and liability is not an effective incentive because behaviour no longer responds to it. In other words, even if the $50 or $500 loss (Reg E) borne by the customer is a valid incentive, the customer will only do the minimum level of precautionary measures necessary. The precautionary measures undertaken do not increase, notwithstanding that the amount lost in the unauthorised payment transaction does. Cooter and Rubin expressly disregard this aspect of moral hazard and argue that it is for this reason that consumers cease to be responsive and that banks should absorb the rest of the losses. They argue since "precaution increases at a decreasing rate" [143] in response to the risk of the transaction, increasing liability becomes oppressive to consumers", and as such, they go on to defend Reg E as it imposes strict liability on the consumer's part at a "significant but not excessive amount".[144]

For unauthorised fraud, there is arguably good reason to adopt this approach and tolerate moral hazard in this sense, for the simple reason that the amount of unauthorised transaction is simply not known to the customers until the customer becomes aware of it, and there is no expectation that customers should increase their precautionary measures in response to unauthorised transactions, the amount of which is wholly out of their control. To that extent, it may well be justified to require banks to bear all losses above a certain threshold. In relation to authorised fraud, however, there is no good reason to accept this sense of moral hazard. This

[141] Robert D. Cooter and Edward L. Rubin, 'Theory of Loss Allocation for Consumer Payments' (1987) 66 Tex L Rev 63.
[142] ibid 90.
[143] ibid 92.
[144] ibid.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

is because customers clearly understand that the default rule is that they have to bear liability on authority terms, and it is common sense that a larger sum of payment instructions naturally comes with a higher risk, and thus, the higher need to take precautions. The flat excess approach under the UK regime effectively removes this inherent sense of precaution in customers and its potential applicability to prevent authorised fraud, especially those involving large sums of payment instructions. Therefore, customer protection – in its broad and blanket terms under the UK regime – does not supply a convincing reason to override the unfairness caused by pinning the bulk of the losses on banks even when they comply with all their duties. Transposing the model for unauthorised fraud for authorised fraud – as the UK regime does – places undue emphasis on the expediency of the loss allocation process (i.e. the loss imposition principle under Cooter and Rubin's framework[145]), and is doctrinally unsound based on this third aspect of moral hazard so conceptualised.

What, then, should be the principle that grounds a loss-sharing approach between customers and banks? The simplest way to preserve the thrust of the factor that 'a larger transaction comes with higher risk' is to share losses on an apportionment basis, e.g. 50:50 split between the customer and the bank as a starting point. That way, the loss allocated to customers and banks will be commensurate with the loss resulting from authorised fraud.

3. The model should allocate more loss to banks when they breach their duties

To the extent reflected in PSD 2 and Reg E,[146] it is central to customer protection that losses for unauthorised fraud may fall on the PSP or financial institution even if it has no fault. This position may be sharply contrasted against the common law position, which provides loss falls upon the customer since there is no claim for breach of duty to fasten liability on the bank,[147] and there is nothing in the contract between a bank and its customer which could require a banker to consider the commercial wisdom of the particular transaction.[148]

Should authorised fraud apply this view of customer protection so enshrined under PSD 2 and Reg E, to override the position under contract or agency law and impose liability on banks even for unauthorised transactions that banks cannot reasonably prevent? The reimbursement duty under the UK regime certainly adopts this view, where PSPs may bear

[145] ibid, 78-84.
[146] See Sections 2.1.1 and 2.1.2.
[147] The position at common law is that, where an unauthorised payment order has been properly authenticated, in the absence of fault by the bank, there may be no common law grounds to fasten liability on the bank, and the customer becomes bound by the properly authenticated payment order regardless of whether or not he has been negligent: Geva, Bank Collections and Payment Transactions (n 26), 397 [7].
[148] *Philipp v Barclays Bank UK plc* (n 1), [3]; *Lipkin Gorman v Karpnale Ltd* [1989] 1 WLR 1340 (CA), 1356.

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

most of the loss subject to the claim excess, even where it has fulfilled its duty to "clearly communicate the PSP's … assessment of the probability that an intended payment is an APP scam payment".[149] But this should not be the case, since customers are *invariably* at fault for authorised fraud. Allocating the bulk of the loss to banks even if they do not breach any duty risks expanding the idea of customer protection too widely.

The better approach is to introduce a cap on the proportion of loss banks have to bear to reflect customer culpability. Following this, if banks are at fault, this is all the more reason why banks should bear *more* loss. This is so, because a breach of duty is significant in theoretical terms, given the trite position under common law that banks have the duty of "reasonable care and diligence in the discharge of user instructions and the performance of all banking functions",[150] or other duties on banks, including the *Quincecare* [151] duty which provides that "a bank has a duty not to execute a payment instruction given by an agent of its customer without making inquiries if the bank has reasonable grounds for believing that the agent is attempting to defraud the customer".[152] This proposal reflects the trite position that banks should compensate for losses naturally arising from their breach of duty. Further, it reflects the advantages of the traditional duty-based view of liability that banks would be incentivised to take measures to prevent authorised fraud and solve moral hazard. Further, the assignment of (more) liability of banks is consistent with Cooter and Rubin's theoretical framework, that liability should be assigned to banks since they can reduce losses at the lowest cost as they can easily innovate by developing technology to reduce fraud losses, respond to legal incentives, and learn the legal rules.[153] At the same time, this proposal partially[154] obviates the direct conflict of the reimbursement duty with the bank's "basic" duty to make payments from the accounts promptly in compliance with the customer's instructions where the customer has so authorised and instructed.[155]

What, then, are the duties of banks that attract increased liability if they are breached? A robust view is that a transaction monitoring duty should be imposed on banks, coupled with the duty (and power) to stop high-risk transactions. The EBA's latest opinion proposed this

[149] UK Dec 2023 Policy Statement (n 6), [5].
[150] Geva, Bank Collections and Payment Transactions (n 26), 397 [7].
[151] *Barclays Bank plc v Quincecare Ltd* [1992] 4 All ER 363.
[152] *Philipp v Barclays Bank UK plc* (n 1), [5].
[153] Cooter and Rubin (n 107), 77.
[154] I say partially, because the very design of the loss allocation model for authorised fraud could be said to contravene the *basic* duty of banks to execute payment transactions.
[155] *Philipp v Barclays Bank UK plc* (n 1), [3].

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

duty.[156] However, the EBA's latest opinion does not suggest that a breach of the transaction monitoring duty would result in PSPs bearing most or all of the losses. Nor does it differentiate between the types of authorised fraud that could be stopped by transaction monitoring and those which could not. As such, penalising banks for their inability to stop fraud by transaction monitoring, which they are incapable of doing so, owing to technological limitations or the very nature of certain types of authorised fraud, is hugely unfair for banks.

In stark contrast to a broad, blanket duty of transaction monitoring, a milder and more nuanced approach could be adopted. Given the ever-evolving typologies of authorised fraud (as elaborated in Section 2.2.2 above), the list of duties of banks should very well be *specific* responses to specific types of authorised fraud. The duty to provide the IBAN/name verification service under PSD 3 to specifically tackle invoice fraud is a good example of this. Regulators may, along similar lines, prescribe a duty on banks to ensure that discrepancies are revealed and that a breach of this duty attracts increased liability. Along these lines, for other types of authorised fraud, duties should be imposed on banks based on what they can (or cannot) do to prevent authorised fraud, in response to the latest state of technological innovations in the payment industry. This allows regulators to tailor nuanced and specific duties to better leverage the role of banks in fighting authorised fraud. Such flexibility is very much in line with the principle – trite and firmly rooted in the bank-customer relationship – that a breach of duty attracts compensation.

4. The model should not provide exceptions for vulnerable customers

The UK regime includes separate provisions for vulnerable customers, based on a presumption that certain customers cannot take reasonable care of authorising transactions. Under the UK regime, vulnerable customers – which is loosely defined as "someone who, due to their personal circumstances, is especially susceptible to harm"[157] – will be compensated even if they are grossly negligent, meaning the *only* pre-fraud duty to have regard to interventions by the PSP and police is waived. In addition, the claim excess is disapplied, meaning that they will be compensated in the entire amount. [158] In effect, even if PSPs succeed in notifying vulnerable customers about the likelihood of the fraud and the vulnerable customer ignores the fraud, PSPs still bear the entire loss. This is problematic since the loss allocation

[156] Under this proposal, if a PSP determines an instant payment is high risk, it can refuse to execute the transaction with proper notification to the PSU, including the reason of the refusal, and the indication of the options available to re-issue the payment order: EBA Opinion (n 49), [29(b)(v)].
[157] Someone who, due to their personal circumstances, is especially susceptible to harm: UK Jun 2023 Policy Statement (n 6), [2.12].
[158] UK Jun 2023 Policy Statement (n 6), [2.11].

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

regime does not penalise the PSP's failure to do all that it can to prevent losses, but rather, imposes liability on the PSP regardless of it.

Such a loose and customer-friendly approach appears to be rather unprincipled and infeasible for wider adoption in other jurisdictions. The definition of vulnerability is arbitrary and unhelpful, coupled with how banks will be reluctant to classify someone as vulnerable due to their limited incentives in doing so.[159] The assumption that vulnerable customers are incapable of taking reasonable care is all the more reason why customers shall listen to the bank's assessment of the likelihood that they are defrauded. Further, it does not appear banks could take any precautionary measures to limit their extent of liability given that it is virtually impossible for banks to ascertain each customer's individual circumstances and determine whether a customer is vulnerable on a case-by-case basis.[160]

Therefore, the model should not provide exceptions for vulnerable customers given that it will likely cause significant confusion.

D. Conclusion and Way Forward

The lack of incentives for the payment industry to take upon the challenge of solving authorised fraud calls for regulators to introduce regulations. I have observed that limits ought to be placed on the loss allocation model to reflect customer fault in authorised fraud. The level of customer liability should be set at a level that sufficiently incentivises customers to take reasonable care in identifying authorised fraud patterns. Further, customers should bear a significant portion of the total loss, and the amount should represent a proportion of the overall loss rather than an upper limit on consumer liability. A breach of duty by banks should continue to inform loss allocation since it incentivises banks to undertake precautionary measures. On that basis, where banks are found to breach their duties, the proportion of loss borne by banks should increase. The precise scope of duty of banks should be tailored to fit the applicable methods to fight specific kinds of authorised fraud, thus, reflecting how banks are best placed to respond to the latest authorised fraud trends and adopt technological innovations to prevent the same. Vulnerable customers ought to be more protected, but in a way that does not remove

[159] As evidenced by how, under the CRM Code, staff of PSPs misses obvious triggers or signs that the customer was vulnerable to the scam, and do not probe further when customers declared a clear vulnerability to the scam which resulted in the scam succeeding: Lending Standards Board, '2022 Review of adherence to Contingent Reimbursement Model Code for Authorised Push Payment Scams – Summary Report' (September 2022) <www.lendingstandardsboard.org.uk/wp-content/uploads/2022/09/CRM-22-Summary-report-Final-0922.pdf> accessed 22 February 2025, 21.

[160] On a related note, it is doubted whether and how a similar measure in the UK regime in relation to the banks' duties after the fraud can work in practice: UK Jun 2023 Policy Statement (n 6), [5.28].

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/

the simple, yet effective means to prevent authorised fraud, namely, the duty to respond to interventions.

Given the dynamic interplay and apparent conflict between policy considerations and theoretical objections, it is not difficult to see why the loss allocation framework for authorised fraud is still in its infancy. Existing proposals tilt the balance in favour of some considerations at the expense of others. Whilst the UK regime weighs overwhelmingly in favour of customer protection, PSD 3 is equally unsatisfactory as it espouses tackling only limited types of authorised fraud. On the other hand, some jurisdictions have decided against any form of loss allocation framework for authorised fraud. One such example is Singapore, which vehemently rejected compensation for authorised fraud as they "do not fundamentally affect confidence in digital payments or digital banking, as they can equally happen in the non-digital world".[161] Other jurisdictions may object to compensation for authorised fraud based on how authority is entrenched as the theoretical foundation. This article proffers a model that solves these problems. It is a principled model that achieves an intricate balance between all considerations presented in this article, which can be a starting point for future empirical and policy research.

It is hoped that authorised fraud shall become a policy priority for regulators. As the UK case shows, customer protection alone can drive regulatory intervention. With reference to broad policy concerns, the model proposed in this article allows regulators to adopt loss allocation rules as they see fit. Regulators may alter the starting point of a 50:50 split and subsequent alteration to a 70:30 split where banks breach their duties, whilst still preventing moral hazard and considering the overarching policy to reduce the social cost of fraud.

[161] Singapore Consultation Paper (n 48), [4.4(a)].

© 2025, The Authors.
This is an open access article distributed under the terms of the Creative Commons Attribution License (CC BY) 4.0 https://creativecommons.org/licenses/by/4.0/