Cambridge Law Review (2025) Vol 10, Issue 2, 61–76

Authorised Push, Institutional Pull: A Critical Appraisal of Competing Priorities in the UK's APP Fraud Reimbursement Regime

CANEL DERYA PARIS ATIK*

ABSTRACT

This article critically examines the competency, scope, and adequacy of the UK's evolving regulatory framework for Authorised Push Payment ('APP') fraud, with a particular focus on the Authorised Push Payment Reimbursement Scheme ('APPRS') introduced under the Financial Services and Markets Act 2023 ('FSMA 2023'). It begins by tracing the statutory underpinnings of the APPRS and situates its emergence within the broader landscape of escalating regulatory efforts to safeguard consumers against socially engineered financial crimes. Subsequently, it turns to the APPRS's structural limitations, including but not limited to jurisdictional exclusions, normatively unjustified reimbursement caps, and ambiguities surrounding the definition and application of the vulnerability exception. It contends that these regulatory gaps undermine both the coherence and fairness of the regime. Furthermore, it unveils and scrutinises the APPRS's reliance on administrative expedience and cost-benefit rationale, which systematically privileges institutional efficiency over the experiential dimensions of harm suffered by fraud victims. The discussion then turns to consider recent legislative amendments to the Payment Services Regulations 2017, which have enabled Payment Service Providers ('PSPs') to withhold payments pre-emptively in the face of suspected fraud. Additionally, it will draw on comparative insights derived from Australia's 'whole-of-ecosystem' approach to appraise the value of, and potential for, cross-sectoral reform in preventing fraud. Ultimately, this article contends that the adequacy of the UK's framework is undermined by two foundational flaws, namely its reactive orientation and its structurally exclusionary design. It concludes that, while the redress mechanism established under the FSMA 2023 represents a meaningful regulatory development, a re-orientation from the UK's ex post, compensation-centric model towards a more preventative, consumer-focused approach, as exemplified by Australian reforms, would offer a more robust and equitable response to APP fraud.

Keywords: financial regulation, authorised push payment fraud, financial law, consumer protection, financial crime

* The author is a penultimate-year Law LLB (Hons) student at the University of Edinburgh and serves as an Editor-in-Chief of the Edinburgh Student Law Review. She expresses her gratitude to her mother, Marjut Vallius, whose willingness to read and comment upon earlier drafts proved invaluable in refining both argument and expression. She further wishes to acknowledge the editorial team, whose thoughtful and discerning engagement has lent greater clarity and coherence to this work.

I. Introduction

In September 2016, the UK's leading consumer advocacy organisation, Which?, filed a super-complaint to the Payment Systems Regulator ('PSR') and the Financial Conduct Authority ('FCA'), calling for a coordinated regulatory response to the escalating threat of 'Authorised Push Payment' ('APP') fraud.[1] The APP classification denotes a distinct form of financial crime, whereby the victim is 'socially engineered into making a bank transfer to a payee/account they consider to be correct, but is in fact in the direct control of a scammer or malicious actor'.[2] Such deception may involve the impersonation of a bank official, the advertisement of fictitious goods, or even the exploitation of an emotional bond preceded by the fabrication of a personal relationship.[3] While the methods vary, the objective remains constant: the fraudulent acquisition of funds through a calculated abuse of confidence.

In response to mounting consumer concern, crystallised by Which?'s super-complaint, the Lending Standards Board introduced the Contingent Reimbursement Model Code in May 2019, which sought to offer redress through voluntary reimbursement obligations for signatory Payment Service Providers ('PSPs').[4] However, its non-mandatory status curtailed its reach, thus leaving customers of non-signatory PSPs vulnerable.[5] To address this regulatory gap, Parliament enacted the Financial Services and Markets Act 2023 ('FSMA 2023'), under which section 72 empowered the PSR to introduce a mandatory reimbursement scheme for victims of APP fraud.[6] Pursuant to this authority, the Authorised Push Payment Reimbursement Scheme ('APPRS') came into force on 7 October 2024 and now constitutes the principal regulatory framework governing APP fraud.[7]

This article will interrogate the scope, structure, and normative coherence of the APPRS, evaluating the extent to which it delivers meaningful protection for victims across a range of circumstances. Section II will outline the legal foundations of the framework, identifying the statutory mechanisms through which reimbursement obligations are imposed. Section III turns to the limitations of the APPRS, asking who is excluded, on what basis, and whether the rationales provided withstand normative scrutiny. It argues that eligibility is governed less by the severity of harm and more by the administrative logic of ease, constraints of enforcement, and elusive efforts at preserving industry stability. Subsequently, Section IV analyses how 'vulnerability' is defined and operationalised within the APPRS, asserting that the lack of definitional clarity substantially compromises its protective function. Moreover, Section V outlines and derives comparative insights from Australia's 'whole-of-ecosystem' ('WOE') model, which has been selected to illuminate the functional merits of its preventative, rather than

[1] Which?, 'Which? Super-Complaint: Consumer Safeguards in the Market for Push Payments' (September 2016) 3–4 <https://www.psr.org.uk/media/t0sln5vn/which-super-complaint-sep-2016.pdf> accessed 31 August 2025.
[2] PwC, 'Authorised Push Payment Fraud: An Uncertain Future' (December 2019) <https://www.pwc.co.uk/financial-services/assets/pdf/authorised-push-payment-fraud-an-uncertain-future.pdf> accessed 31 August 2025.
[3] Lending Standards Board, 'Information for Customers on the Contingent Reimbursement Model Code for APP Scams (the CRM Code)' (2022) 3 <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2022/01/Information-for-customers-CRM.pdf> accessed 31 August 2025.
[4] ibid.
[5] Jo Braithwaite, '"Authorized Push Payment" Bank Fraud: What Does an Effective Regulatory Response Look Like?' (2024) 10 Journal of Financial Regulation 174, 181–83.
[6] Financial Services and Markets Act 2023 ('FSMA 2023'), s 72(1).
[7] PSR, 'Policy Statement: Fighting Authorised Push Payment Scams: Final Decision' (PS23/4, December 2023) ('Policy Statement PS23/4') 3 <https://www.psr.org.uk/media/kwlgyzti/ps23-4-app-scams-policy-statement-dec-2023.pdf> accessed 31 August 2025.

remedial, focus. It then considers recent amendments to the Payment Services Regulations 2017, recognising their potential to enable ex ante intervention, as well as the 'failure to prevent fraud' offence instituted by the Economic Crime and Corporate Transparency Act 2023 ('ECCTA 2023'). Taken together, these domestic developments indicate an expanding legislative willingness to impose liability, not merely where corporations have commissioned fraud, but also where they have neglected to prevent it. Yet, despite signalling progress, these innovations remain structurally isolated, thus accentuating the need for analogous reforms in the domain of APP fraud.

Cumulatively, these sections demonstrate that, although the APPRS marks a notable regulatory advancement, it continues to exclude categories of victims whose exclusion cannot be normatively justified. In privileging institutional pragmatism over inclusive protection, the APPRS risks replicating the very inequities it was introduced to redress. Moreover, this article will argue that the aforementioned exclusions are not simply administrative oversights; they are symptomatic of a framework that remains reactive by design. This article contends that, to fulfil its protective mandate, the APPRS must evolve into a model that not only compensates after harm has occurred, but also anticipates, disrupts, and deters the conditions through which such harm is made possible.

II. The Legal Foundations

As stipulated under section 72(1) of the FSMA 2023, the PSR is required to 'prepare... a relevant requirement for reimbursement in such qualifying cases of payment orders as the regulator considers should be eligible'.[8] In defining a 'qualifying case', section 72(2)(b) of the FSMA 2023 specifies that the payment order must have been executed subsequent to fraud or dishonesty,[9] while section 72(2)(a) narrowly restricts such cases to transactions executed via the Faster Payments Scheme ('FPS').[10] By restricting statutory coverage to FPS transactions, section 72(2)(a) raises 'prima facie' concerns as to the equity and universality of the APPRS's protective function, particularly in the light of the growing prevalence of cross-platform transfers and alternative payment systems in contemporary financial crime.[11]

Moreover, sections 54 and 55 of the Financial Services (Banking Reform) Act 2013 authorise the PSR to issue 'directions' to participants in regulated payment systems.[12] Directions may either 'require or prohibit the taking of specified action in relation to the system' (section 54(2)(a)) or 'set standards to be met in relation to the system' (section 54(2)(b)). Thus, the PSR issued the following legal instruments to operationalise its mandate under section 72:

1. A specific requirement ('SR1'), imposed via section 55(1), obliging Pay.UK (the FPS's payment system operator) to ensure that its FPS rules include a

[8] FSMA 2023, s 72(1).
[9] ibid s 72(2)(b).
[10] ibid s 72(2)(a).
[11] The Payments Association, 'The Impact of APP Fraud on Cross-Border Payments' (2024) 10 <https://thepaymentsassociation.org/wp-content/uploads/2024/09/The-impact-of-APP-fraud-on-cross-border-payments-1.pdf> accessed 31 August 2025.
[12] Financial Services (Banking Reform) Act 2013, s 54(1).

reimbursement requirement for APP fraud payments executed over the FPS;[13]

2. A specific direction ('SD19'), pursuant to section 54(1)–(2), requiring Pay.UK to implement a compliance monitoring regime to ensure the effective and consistent enforcement of reimbursement rules across PSPs;[14] and
3. A specific direction ('SD20') issued under section 54(1)–(2) to all relevant PSPs, mandating their compliance with the reimbursement rules as a condition of their participation in the APPRS.[15]

Principally, the FPS Reimbursement Requirement obliges Sending PSPs ('SPSP') to reimburse APP fraud victims in full, contingent on the payment falling within the scope of the FPS Reimbursement Rules.[16] Once the customer submits their claim, the SPSP must transfer the 'Reimbursable Amount' ('RA') to the customer within five business days of receipt of the claim, subject only to the potential invocation of the 'stop the clock' provision, which allows SPSPs to request further information concerning the validity of the claim.[17] The SPSP must conclude whether or not the claim will be reimbursed by the end of the thirty-fifth business day as of the claim submission date.[18] Once the RA has been calculated, the Receiving PSP ('RPSP') must transfer half of the total RA to the SPSP.[19] The regulatory instruments that operationalise the FPS Reimbursement Requirement constitute a laudable advancement in consumer protection. Nonetheless, they remain grounded in a proceduralised conception of harm and redress that stands at odds with the nuanced, experiential realities of APP fraud, a point of tension that will be examined in greater depth in Section III below.

III. Examining the Scope of Reimbursable Claims: Incomplete Universality

A. Structural limitations and undue exclusions

Under the FPS Reimbursement Rules, claims must refer to a 'relevant account'.[20] This must be a UK-based account capable of sending or receiving payments via FPS; it cannot, however, be an account provided by a credit union, municipal bank, or national savings bank.[21] Furthermore, a singular claim cannot exceed the maximum level of reimbursement ('MLR'), which

[13] PSR, 'Specific Requirement 1 on the Faster Payments Operator to Insert APP Scam Reimbursement Rules into the Faster Payments Scheme Rules' (July 2024) 3 <https://www.psr.org.uk/media/xenefhgp/amended-specific-requirement-1-july-2024-corrected.pdf> accessed 31 August 2025.

[14] PSR, 'Specific Direction 19 Imposing Certain Responsibilities on the Faster Payments Operator in Respect of the Faster Payments Scheme APP Scam Reimbursement Rules' (July 2024) 3 <https://www.psr.org.uk/media/cbrcixgu/amended-specific-direction-19-july-2024.pdf> accessed 30 August 2025.

[15] PSR, 'Specific Direction 20 to PSPs Participating in the Faster Payments Scheme that Provide Relevant Accounts, to Reimburse FPS APP Scam Payments and Comply with the Reimbursement Rules' (July 2024) 3 <https://www.psr.org.uk/media/rqrpnb0w/amended-specific-direction-20-july-2024.pdf> accessed 30 August 2025.

[16] Pay.UK, 'FPS Reimbursement Rules' (4 December 2024) 6 <https://www.wearepay.uk/wp-content/uploads/2024/12/FPS-Reimbursement-Rules-Schedule-4.pdf> accessed 31 August 2025.

[17] ibid.

[18] ibid 11.

[19] ibid 14.

[20] PSR, 'Policy Statement PS23/4' (n 7) 17.

[21] Pay.UK (n 16) 25.

is presently set at £85,000.[22] SPSPs may also impose a claim excess of £100 on non-vulnerable consumers,[23] aimed at disincentivising 'morally hazardous behaviour' and encouraging greater consumer caution in high-risk transactions.[24] The foregoing criteria reveal three key structural limitations embedded in the current framework: a jurisdictional limitation (linked to the UK); a payment-system limitation (tied to the FPS); and an institutional limitation (excluding certain financial providers). Each raises concerns about the APPRS's coherence and fairness, which the subsequent analysis will consider in turn. For present purposes, 'fairness' is to be understood as the equilibrium struck between two competing imperatives: on one hand, the 'consumer interest' in being shielded from undue loss and, on the other, the 'systemic interest' in promoting the efficiency of, and maintaining stability within, the financial sector. Within these conceptual bounds, a policy may be deemed 'unfair' where it disproportionately impinges upon one interest, in the absence of a countervailing justification proportionate to the weight that it displaces.

Significantly, a victim of APP fraud falls within the scope of the APPRS only where both the sending and receiving accounts are held within the UK.[25] This effectively excludes victims of cross-border fraud, irrespective of the sophistication or scale of the deception involved. This omission is striking given that UK Finance's 2024 data has underscored the growing significance of this category: international payments were identified as the second most-affected payment method, surpassed only by domestic FPS transactions in both volume and value.[26] In 2023 alone, 3,302 cross-border APP fraud payments were recorded, with total losses amounting to £25.9 million.[27] Notably, the PSR has not offered public justification for excluding such payments from the APPRS's scope. One may reasonably infer that the decision is underpinned by the difficulty of securing reimbursement from extra-jurisdictional financial institutions not subject to UK regulatory authority. As The Payments Association notes, effective cross-border fraud prevention may require more than regulatory intervention alone; it may necessitate coordinated industry initiatives, bilateral enforcement protocols, and reform of data-sharing legislation.[28] It is thus apparent that the PSR is not in a position to effect the necessary changes unilaterally, given the indispensable role of international cooperation. The feasibility and architecture of the international cooperation required to effect such change, and the question of which actors might be responsible for effecting it, lie beyond the remit of this article. Of greater significance for present purposes is the distribution of liability, where the involvement of an international recipient of the fraudulently obtained funds effectively provides SPSPs with an unearned immunity from liability. Thus, even recognising the aforesaid constraints, the total absence of a redress mechanism for victims of cross-border APP fraud remains problematic. Intuitively, an alternative model presents itself: the victim could still be reimbursed by the SPSP, with the receiving institution's contribution omitted.

[22] PSR, 'Policy Statement: Faster Payments APP Scams Reimbursement Requirement: Confirming the Maximum Level of Reimbursement' (PS24/7, October 2024) ('Policy Statement PS24/7') 3 <https://www.psr.org.uk/media/e30pwlly/ps24-7-app-scams-maximum-level-of-reimbursement-policy-statement-oct-2024.pdf> accessed 30 August 2025.

[23] PSR, 'Policy Statement PS23/4' (n 7) 32.

[24] ibid.

[25] Pay.UK (n 16).

[26] UK Finance, 'Annual Fraud Report 2024' (2024) 61 <https://www.ukfinance.org.uk/system/files/2024-06/UK%20Finance%20Annual%20Fraud%20report%202024.pdf> accessed 31 August 2025.

[27] ibid.

[28] The Payments Association, 'The Impact of APP Fraud' (n 11) 33.

Though imperfect, such a model would at least ensure partial compensation and preserve the core principle of shifting absolute liability away from victims. That such a solution remains unexplored suggests that institutional expedience has been prioritised over equitable design.

A similar critique applies to the exclusion of non-FPS transactions. For present purposes, APP scams executed over the Clearing House Automated Payment System ('CHAPS'), a high-value payment system operated by the Bank of England, are excluded from analysis; they are covered by their own, parallel APP fraud reimbursement requirement.[29] This is supported by Specific Direction 21 ('SD21'), a mirror direction of SD20, which applies to CHAPS PSPs and amends the rules applicable to CHAPS transactions.[30] According to 2023 data, 7,477 non-FPS and non-CHAPS payments were affected by APP fraud, resulting in total losses of £56.4 million.[31] While these transactions constitute a relatively small proportion of the 417,459 total fraud cases reported that year,[32] their exclusion nonetheless reinforces a fragmented model of protection. Once more, it is a structural consideration (namely, the payment's pathway), rather than the gravity of the injury, which determines the consumer's eligibility for redress. A final limitation arises from the exclusion of accounts held with exempted institutions, effectively leaving a subset of consumers without access to redress based purely on their institutional affiliation. The PSR has cited the comparatively low incidence of APP fraud within these institutions as a justification for the carve-outs, arguing that the practical burden of compliance outweighs the benefits of inclusion.[33] Supporting this rationale, 2022 data reported only 41 cases with a combined value of £17,000.[34]

Considered cumulatively, these exclusions raise substantive concerns regarding the internal coherence and distributive fairness of the APPRS. The PSR's fractured policy orientation may be better understood through Julia Black's observation that regulatory organisations selectively respond to 'legitimacy claims' based on their strategic priorities and dependencies.[35] Black contends that regulators may dismiss a legitimacy claim where it does not serve their core objectives, is inessential to their survival, or is eclipsed by a competing claim from a more influential 'legitimacy community'.[36] Applied to the present facts, consumer communities advocating for greater fraud protections represent the subordinate 'legitimacy claim', whereas PSPs and financial institutions, seeking to limit financial liability and protect profit margins, exert the dominant claim. The APPRS's architecture reflects this hierarchy, whereby institutional stability and industry competitiveness take precedence over comprehensive consumer protection.

Furthermore, Black maintains that regulators are more responsive to claims raised by entities on which they are highly dependent or with whom they are structurally interdependent.[37] This may explain the PSR's repeated privileging of industry interests; as Tim Yi Jane

[29] PSR, 'Policy Statement: Fighting Authorised Push Payment Scams: CHAPS APP Scams Reimbursement Requirement' (PS24/5, September 2024) 3 <https://psr.org.uk/media/th4jea5a/ps24-5-app-scams-chaps-reimbursement-sept-2024.pdf> accessed 1 September 2025.

[30] PSR, 'Specific Direction 21 to PSPs Participating in CHAPS that Provide Relevant CHAPS Accounts, to Reimburse CHAPS APP Scam Payments and Comply with the CHAPS Reimbursement Rules' (September 2024) 4 <https://www.psr.org.uk/media/yxbh4dvt/specific-direction-21-chaps-reimbursement-september-2024.pdf> accessed 1 September 2025.

[31] UK Finance, 'Annual Fraud Report' (n 26).

[32] ibid.

[33] PSR, 'Policy Statement PS23/4' (n 7) 16.

[34] ibid.

[35] Julia Black, 'Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes' (2008) 2 Regulation & Governance 137, 154.

[36] ibid.

[37] ibid 156.

Ngan notes, PSPs retain a degree of structural and financial influence within the regulatory ecosystem that consumers are ill-equipped to counter.[38] Notably, the Treasury Committee, in its review of the APPRS's early implementation, expressed concern over the PSR's decision to delegate operational responsibility to Pay.UK, an industry body both funded and guaranteed by the very institutions it would ultimately regulate.[39] Although it is an ordinary feature of legal redress mechanisms that access is circumscribed by design, such limitations are customarily justified on functional or principled grounds. By contrast, the APPRS deviates from this rationale, systemically privileging institutional convenience and regulatory dependencies, considerations far removed from the consumer experience, while relegating what should be central to the inquiry: the merits of the claim and the sophistication of the fraud. The outcome is a scheme whose claims to fairness and coherence are necessarily weakened.

B. The Maximum Level of Reimbursement

One of the most contentious features of the APPRS is the MLR, which, despite initial proposals of £415,000, was ultimately set at £85,000 in October 2024.[40] In defence of this reduction, the PSR noted that 99.8 per cent of FPS transactions by volume and 90 per cent by value would remain covered.[41] The justification concentrated on potential 'prudential risks' to PSPs, namely that a higher MLR may deter investment within the sector, jeopardise the survival of smaller firms, and undermine industry competitiveness.[42] Crucially, the PSR's rationale relied on a cost-benefit analysis ('CBA') conducted in support of the reimbursement framework. Such analyses, by design, are grounded in utilitarian logic: they seek to maximise net benefit for the greatest number, typically by aggregating outcomes in economic terms.[43]

However, as the Financial Services Consumer Rights Panel has noted, this method systematically privileges quantifiable metrics over qualitative dimensions of harm, such as emotional distress, erosion of personal dignity, or the loss of financial security, which are less easily reduced to monetary value.[44] Such concerns are corroborated by the verifiable correlation between fraud victimisation and psychological harm: 70 per cent of victims reported heightened stress, 60 per cent noted mental health decline, and 50 per cent experienced a deterioration in their financial well-being.[45] Moreover, the Panel criticised the PSR's industry-

[38] Tim Yi Jane Ngan, 'Response to CP24/11 – "Faster Payments APP Scams: Changing the Maximum Level of Reimbursement"' (2024) 8 <https://pure.manchester.ac.uk/ws/portalfiles/portal/344733017/Response_to_PSR_consultation_CP24-11_-_FINAL_v2.pdf> accessed 1 September 2025.

[39] House of Commons Treasury Committee, 'Scam Reimbursement: Pushing for a Better Solution' (HC 989, 6 February 2023) 17–18.

[40] PSR, 'Policy Statement PS24/7' (n 22).

[41] ibid 20.

[42] ibid 24.

[43] See Elliot Marseille and James G Kahn, 'Utilitarianism and the Ethical Foundations of Cost-Effectiveness Analysis in Resource Allocation for Global Health' (2019) 14(1) Philosophy, Ethics, and Humanities in Medicine <https://doi.org/10.1186/s13010-019-0074-7> accessed 1 September 2025.

[44] Letter from Helen Charlton (18 September 2024) 3–4 <https://www.fca.org.uk/panels/consumer-panel/publication/20240918_final_fscp_response_to_cp24.11_faster_payments_app_scams_-_changing_the_maximum_level_of_reimbursement.pdf> accessed 1 September 2025.

[45] The findings, which were published by Which?, derived from a survey of 1,012 adult fraud victims: see 'Fraud Has a Lasting Impact on Victims' Mental Health, Which? Warns' (*Which?*, 12 September 2024) <https://www.which.co.uk/policy-and-insight/article/fraud-has-a-lasting-impact-on-victims-mental-health-which-warns-aLkJY1z7wrfu> accessed 1 September 2025.

sympathetic policy orientation, citing the accelerating frequency of high-value fraud and challenging the PSR's dismissal of the issue on account of its statistical insignificance in the broader sphere of financial crime.[46] In pursuing a purely quantitative analysis, the PSR effectively excluded victims of high-value fraud, whose losses may be financially and psychologically catastrophic, despite being statistically marginal.

While a strictly quantitative CBA may appear methodologically sound and economically rational, it risks erasing the practical gravity of outlier cases under the guise of statistical optimisation. Within such a framework, 411 incidents may appear statistically negligible. However, victims of high-value fraud (for example, conveyancing fraud) frequently experience traumatic and deeply disruptive effects both financially and psychologically, with experts advising that the emotional ramifications may be more enduring than the financial losses.[47] Notably, 'several' victims have suffered losses of £250,000[48] and even as high as £640,000.[49] Although comprehensive research on the long-term effects of high-value APP fraud remains limited, consumer advocacy organisations have begun to document the underlying human cost. Action Fraud, for instance, reported that an unnamed individual defrauded of £640,000 experienced a 'devastating life-long impact', including the non-recovery of personal savings and equity, with grave implications for their financial stability and well-being.[50] As William W May cautions, the blanket exclusion of unquantifiable harms from a CBA risks endorsing outcomes that inflict injury or are otherwise ethically contentious.[51] By disregarding the profound psychological trauma endured by victims of high-value fraud, the PSR's exclusively quantitative CBA arrived at a conclusion that, while procedurally sound, reflects a troubling disregard for human impact and is therefore conceptually flawed. Moreover, if, as the PSR maintains, such cases are indeed rare, then the practical cost of covering them may be far less burdensome to PSPs than has been suggested.[52]

Additionally, the PSR has pointed to the Financial Ombudsman Service ('FOS') as an alternative avenue of redress, noting that consumers may be awarded between £430,000 and £945,000 if they can demonstrate that the SPSP, the RPSP, or both were at fault for the fraud's success.[53] While the mechanism remains a valuable safeguard, its efficacy is undermined in practice: the FOS's uphold rate[54] for APP fraud complaints is now at its lowest in

[46] Letter from Helen Charlton (18 September 2024) (n 44). The claims referred to may be observed at PSR, 'Policy Statement PS24/7' (n 22) 29.

[47] See Suleman Lazarus and Liz Ziegler, 'What Is the Emotional Impact of Fraud?' (*Lloyds Banking Group*, 5 December 2024) <https://www.lloydsbankinggroup.com/insights/what-is-the-emotional-impact-of-fraud.html> accessed 31 August 2025.

[48] 'Lloyds Bank Warns of Worrying Rise in Conveyancing Fraud' (*Lloyds Banking Group*, 18 June 2024) <https://www.lloydsbankinggroup.com/media/press-releases/2024/lloyds-bank-2024/lloyds-bank-warns-of-worrying-rise-in-conveyancing-fraud.html> accessed 31 August 2025.

[49] Action Fraud, 'Can You Afford to Lose Your Entire Deposit or Purchase Money?' (2022) <https://data.actionfraud.police.uk/cms/wp-content/uploads/2022/03/2b.-Conveyancing_Leaflet.pdf> accessed 1 September 2025.

[50] ibid.

[51] William W May, '$s for Lives: Ethical Considerations in the Use of Cost/Benefit Analysis by For-Profit Firms' (1982) 2 Risk Analysis 35, 46.

[52] PSR, 'Policy Statement PS24/7' (n 22) 15.

[53] ibid 18.

[54] FOS, 'Temporary Changes to Outcome Reporting in Our Business-Specific Complaints Data' (March 2023) 2 <https://www.financial-ombudsman.org.uk/files/324180/Financial-Ombubsman-Service-Temporary-changes-to-outcome-reporting-in-our-business-specific-complaints-data.pdf> accessed 31 August 2025 (defining the 'uphold rate' as 'the percentage of resolved complaints where we find in favour of the complainant... The "uphold rate" reflects the percentage of complaints resolved as "change in outcome".').

three years, having declined from 54 per cent in 2022 to just 37 per cent in 2025.[55] Accordingly, the availability of redress through the FOS does little to offset the structural inequities embedded within the current reimbursement framework. Moreover, even for victims with a higher likelihood of success, pursuing redress through the FOS entails considerable delays and procedural strain. According to FOS data, only 24 per cent of APP fraud cases are resolved within three months, 46 per cent within six, and over half extend beyond that period.[56] These figures compare unfavourably to resolution times for other fraud classifications, where 41 per cent are resolved within three months and 67 per cent within six.[57]

Thus, to clarify, the average victim of APP fraud not only faces a 63 per cent likelihood of denial, but also a 76 per cent chance of waiting over three months, and a 54 per cent chance of waiting beyond six. It ought to be emphasised that the preceding analysis does not purport to attribute the observed decline in the FOS's uphold rate to the proliferation of APP fraud, nor to any lack of institutional commitment on behalf of the FOS. Rather, the reduced success rate may, as a possibility, reflect a higher incidence of non-qualifying claims or findings of consumer negligence, for instance, where exceptions, such as the Consumer Standard of Caution Exception ('CSCE') (addressed below) are engaged. For present purposes, the point remains that the FOS's efficacy as a viable compensatory mechanism is empirically limited, thus rendering the PSR's confidence in it not merely optimistic, but largely unsubstantiated.

IV. The Consumer Standard of Caution Exception: Vulnerability in Practice

Under the APPRS, consumers may be denied reimbursement if they are found to have acted 'fraudulently' or with 'gross negligence', a principle known as the 'CSCE'.[58] However, this exclusion does not apply to consumers deemed 'vulnerable'.[59] To meet the standard of caution, consumers are expected to:

1. Respond appropriately to warnings issued by their PSP or relevant authorities regarding the risk of fraud;
2. Report the incident promptly upon acquiring actual or constructive knowledge of the fraud (no later than 13 months after the payment was made);
3. Cooperate with reasonable and proportionate information requests, and where prompted;
4. Either consent to their PSP filing a police report or file one themselves.[60]

[55] Letter from James Dipple-Johnstone to Dame Meg Hillier (13 March 2025) 4 <https://committees.parliament.uk/publications/47242/documents/244869/default/> accessed 1 September 2025.
[56] ibid 5.
[57] ibid 4.
[58] See PSR, 'Guidance: Authorised Push Payment Fraud Reimbursement: The Consumer Standard of Caution Exception Guidance' (December 2023) 2 <https://www.psr.org.uk/media/as3a0xan/sr1-consumer-standard-of-caution-guidance-dec-2023.pdf> accessed 1 September 2025.
[59] ibid.
[60] ibid.

Significantly, the onus rests on the PSP to demonstrate that a consumer has conducted themselves with gross negligence,[61] defined by the PSR as a 'significant degree of carelessness'.[62] This high evidentiary threshold is a welcome consumer-facing protection, designed to incentivise PSPs to invest in their fraud prevention mechanisms.[63]

Nonetheless, the practical application of the CSCE raises critical concerns, particularly surrounding the scope and interpretation of the vulnerability exception. The key issue lies in the operationalisation of vulnerability, namely whether the PSR's guidance provides sufficient clarity to ensure fair and consistent treatment of vulnerable consumers by PSPs. Notably, the PSR has adopted the FCA's operational definition of vulnerability, whereby a vulnerable customer is characterised as '[s]omeone who, due to their personal circumstances, is especially susceptible to harm – particularly when a firm is not acting with appropriate levels of care'.[64] Furthermore, the definition is substantiated by four core characteristics: (a) health conditions that impair one's ability to engage in day-to-day activities; (b) debilitating life events (for example, bereavement, unemployment, or relationship breakdown); (c) low emotional or financial resilience; and (d) limited capability (for example, poor financial or digital literacy).[65]

Thus, the FCA's framework is both comprehensive and consumer-oriented, thereby rendering it well suited for application within the APPRS. However, the PSR's accompanying guidance has stated that PSPs 'should' examine each consumer's circumstances on a case-by-case basis to gauge the extent to which their particular characteristics, whether tentative or enduring, led them to be defrauded.[66] Of even greater concern is the PSR's failure to provide any further guidance on how PSPs should assess vulnerability in a way that avoids discriminatory or inconsistent outcomes. Crucially, it offers no further detail on which characteristics increase susceptibility to fraud or how these should be weighed in PSPs' assessments. This omission introduces an elusive degree of discretion, granting PSPs significant interpretive latitude in determining who qualifies for protection, and potentially leading to inconsistent outcomes.

Notably, previous examples demonstrate that detailed regulatory guidance has enhanced the industry's understanding of how vulnerable consumers should be identified and supported. In 2021, the FCA issued specific and actionable guidelines on the treatment of vulnerable customers,[67] protections that are now reinforced by the obligations introduced under the newly-instituted Consumer Duty.[68] According to the FCA's post-implementation evaluations, the guidance has positively influenced firms' engagement with vulnerable consumers. In particular, firms praised the 'clarity' of the guidance, especially its articulation of the drivers

[61] ibid 3.
[62] ibid.
[63] PSR, 'Policy Statement PS23/4' (n 7) 28.
[64] ibid 37 (emphasis removed).
[65] FCA, 'Finalised Guidance: FG21/1 Guidance for Firms on the Fair Treatment of Vulnerable Customers' (February 2021) 9 <https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf> accessed 1 September 2025. According to the FCA, 52 per cent of UK adults fall within at least one of these categories, thus reinforcing the breadth and relevance of this definition: see FCA, 'Financial Lives 2022: Key Findings from the FCA's Financial Lives May 2022 Survey' (26 July 2023) 90 <https://www.fca.org.uk/publication/financial-lives/financial-lives-survey-2022-key-findings.pdf> accessed 31 August 2025.
[66] PSR, 'Policy Statement PS23/4' (n 7) 37.
[67] See FCA, 'Finalised Guidance' (n 65).
[68] FCA, 'Firms' Treatment of Customers in Vulnerable Circumstances – Review' (*Financial Conduct Authority*, 7 March 2025) <https://www.fca.org.uk/publications/multi-firm-reviews/firms-treatment-vulnerable-customers> accessed 1 September 2025.

and characteristics of vulnerability, reporting that it meaningfully improved their ability to deliver appropriate support.[69] Moreover, the FCA's evaluations note that the guidance has contributed to cultural shifts within firms, fostering greater awareness of, and sensitivity to, consumer vulnerability.[70] This conclusion remains the FCA's own and should not be taken to represent the views of the industry as a whole. Nonetheless, the finding has been extrapolated from a multi-firm survey of 725 respondents, thus lending it a degree of empirical legitimacy.[71] By contrast, the PSR, having neglected to provide binding criteria for assessing vulnerability, has effectively delegated interpretive control to PSPs, the very institutions with a vested interest in limiting liability. This imbalance contradicts the consumer-centric principles underpinning the FCA's vulnerability framework[72] and creates scope for arbitrary or inconsistent decision-making, thereby casting doubt on the adequacy of the current regulatory regime.

V. A Cross-Jurisdictional Case Study

In addition to reforms introduced under the FSMA 2023, new UK legislation has empowered PSPs to delay the execution of outbound payments where there are legitimate grounds for suspicion of fraud. Under the prior framework, governed by regulation 86(1) of the Payment Services Regulations 2017, a payee's PSP was obliged to credit the payment amount to the recipient's account by the close of the next business day, following receipt of the payment order.[73] While this regime unequivocally enhanced transactional expediency, it arguably did so at the expense of consumer protection and institutional accountability, thus reinforcing a paradigm of automaticity that left limited scope for intervention in the face of suspected fraud. To remedy this gap, the Payment Services (Amendment) Regulations 2024 provided PSPs with an ex ante right of intervention, allowing them to delay crediting the relevant amount where there are 'reasonable grounds to suspect a payment order… has been placed subsequent to fraud or dishonesty perpetrated by a person other than the payer'.[74] The execution of the order may be deferred for four business days,[75] where the delay must serve the specific purpose of enabling the PSP to contact the payer or an appropriate third party to ascertain whether the order ought to be fulfilled.[76] This initiative marks a welcome shift towards a more preventative regulatory posture, one that recognises the importance of disrupting fraud prior to its materialisation, rather than relying solely on mechanisms of retrospective redress.

With that being said, the measure remains a narrowly framed tool within a largely reactive framework. Moreover, as industry stakeholders have contended, it may be unjust to expect financial institutions to bear sole responsibility for consumer reimbursement where

[69] ibid.
[70] ibid.
[71] ibid.
[72] See FCA, 'Finalised Guidance' (n 65) 3, which states the FCA's stated objective as follows: 'Ensuring consumers have an appropriate degree of protection is central to what the FCA does. This includes protecting vulnerable consumers. We want vulnerable consumers to experience outcomes as good as those for other consumers and receive consistently fair treatment across the firms and sectors we regulate.'
[73] Payment Services Regulations 2017, SI 2017/752 ('PSRs 2017'), reg 86(1).
[74] ibid reg 86(2A)(a), inserted by the Payment Services (Amendment) Regulations 2024, SI 2024/1013 ('PSAR 2024'), reg 2(4)(b).
[75] PSRs 2017, reg 86(2C), inserted by PSAR 2024, reg 2(4)(b).
[76] PSRs 2017, reg 86(2B), inserted by PSAR 2024, reg 2(4)(b).

the fraudulent transactions originated on online platforms, search engines, or telecommunications networks.[77] This concern is empirically grounded: according to UK Finance, 76 per cent of fraud cases now originate online.[78] Why, then, are other corporate facilitators not being held accountable? A notable point of contrast may be drawn from Australia's emerging WOE approach,[79] internationally recognised for its emphasis on coordinated prevention, shared responsibility, and systemic intelligence-sharing.[80] As Anna Bligh, the CEO of the Australian Banking Association, has emphasised, a truly robust approach towards consumer protection must engage more deeply with how victims become victimised in the first place.[81]

For the purposes of the subsequent analysis, Australia has been selected as the principal comparator. This choice is attributable, not to the relative sophistication of its financial services sector, where a jurisdiction like Singapore might appear to be the more obvious candidate, but rather to the breadth and structural sophistication of Australia's Scams Prevention Framework ('SPF'). Unlike Singapore's Shared Responsibility Framework ('SRF'), which is articulated only through regulatory Guidelines (administered by the Monetary Authority of Singapore and the Infocomm Media Development Authority) and applicable only to financial institutions and telecommunications providers,[82] the SPF retains its footing in statute[83] and is universally applicable across the Australian regulated economy.[84] Moreover, whereas the SRF targets primarily 'phishing scams'[85] and excludes APP fraud on the basis that it involves consumer authorisation,[86] the SPF expressly captures APP fraud within its broader regulatory design.[87] On the aforesaid premises, the Australian model represents the most analytically rich and practically instructive comparator for UK policymakers.

Central to Australia's strategy is the National Anti-Scam Centre ('NASC'), a government-led body launched in July 2023. It brings together public and private stakeholders, including PSPs, law enforcement agencies, telecommunications providers, and digital platforms

[77] The Payments Association, 'Faster Payments APP Scams: Changing the Maximum Level of Reimbursement: Response from the Payments Association' (September 2024) 5 <https://thepaymentsassociation.org/wp-content/uploads/sites/7/2024/09/TPA-Response-to-PSR-CP24-11-V4-0-FINAL.pdf> accessed 1 September 2025.

[78] UK Finance, 'Annual Fraud Report' (n 26) 21.

[79] Australian Government Treasury, 'Scams Prevention Framework: Summary of Reforms' (September 2024) 4 <https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-summary.pdf> accessed 1 September 2025.

[80] The Payments Association, 'The Impact of APP Fraud' (n 11) 31.

[81] Anna Bligh, 'Why Australian Banks Are Better at Stopping Scammers Than British Banks' *The Age* (24 August 2024) <https://www.theage.com.au/national/why-australian-banks-are-better-at-stopping-scammers-than-british-banks-20240821-p5k443.html> accessed 1 September 2025.

[82] See Monetary Authority of Singapore and Infocomm Media Development Authority, 'Guidelines on Shared Responsibility Framework' (2024) 1 <https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/pso/guidelines-on-shared-responsibility-framework/guidelines-on-shared-responsibility-framework.pdf> accessed 31 August 2025.

[83] See Scams Prevention Framework Bill 2025 (Cth).

[84] Claudine Salameh and Tamsyn Sharpe, 'Combatting Scams in Australia, Singapore, China and Hong Kong' (*K&L GATES*, 17 April 2025) <https://www.klgates.com/Combatting-Scams-in-Australia-Singapore-China-and-Hong-Kong-4-17-2025> accessed 31 August 2025.

[85] 'Combatting Scams' (*Monetary Authority of Singapore*) <https://www.mas.gov.sg/regulation/combatting-scams> accessed 30 August 2025. The Monetary Authority of Singapore defines a 'phishing scam' as 'a way of obtaining sensitive personal information such as one's banking account details, PIN, one-time passwords (OTP), credit card number, user ID or password through the Internet, in order to perform unauthorised banking transactions': Monetary Authority of Singapore, 'Annex B' <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Press-Releases/Annex-B--Tips-to-guard-against-phishing-activities.pdf> accessed 30 August 2025.

[86] Monetary Authority of Singapore and Infocomm Media Development Authority (n 82) 1, 4. For a detailed overview of the respective fraud typologies captured by the Singaporean SRF and the Australian SPF, see further nn 82, 85 above.

[87] Australian Government Treasury, 'Scams Prevention Framework: Protecting Australians from Scams' (January 2025) 3 <https://treasury.gov.au/sites/default/files/2025-01/p2025-623966.pdf> accessed 1 September 2025.

within a unified scam prevention infrastructure.[88] Central to the Australian model is the view that fraud prevention is a collective responsibility throughout the scam lifecycle.[89] Rather than placing the burden exclusively on consumers or financial institutions, it imposes minimum obligations and potential liabilities on all relevant parties, acknowledging that scams are facilitated by an interconnected network of digital, financial, and communicative enablers.[90] For instance, Australian regulators have enforced the 'Reducing Scam Calls and Scam Short Messages (SMs) Code', which obliges telecommunications providers to take reasonable steps to detect and block scam communications.[91] Since its implementation, 2.3 billion scam calls and 857.4 million fraudulent messages have been blocked.[92] While UK regulation allows PSPs to delay payments on suspicion of fraud, Australia mandates cross-sectorial, intelligence-led responses, allowing for real-time data-sharing and malicious website takedowns.[93] Within its first year, the NASC has removed over 7,300 scam-linked domains.[94]

Moreover, the Australian legislature has taken concrete steps to codify the WOE model into law, offering valuable lessons for UK policymakers. On 13 February 2025, the Federal Parliament passed the Scams Prevention Framework Bill 2025,[95] which established an overarching regulatory structure applicable across sectors. The Australian Competition and Consumer Commission will spearhead its implementation,[96] with the authority to impose either economy-wide 'overarching principles' or targeted 'sector-specific codes' on regulated industries.[97] These instruments will pursue the core objectives of preventing, detecting, and disrupting fraud, while also ensuring that it is adequately responded to and reported.[98] Sector-specific codes will outline minimum, industry-specific compliance obligations[99] and are initially expected to be applied to telecommunications, banking, digital platforms (including social media), search engines, and direct messaging services.[100] However, the SPF is an innately 'adaptable' and 'responsive' tool.[101] Its 'adaptability' is operationalised through the discretionary powers conferred upon the Treasury Minister, who may designate additional sectors as regulated where necessary, ensuring that no actor within the fraud-enabling ecosystem can evade regulatory accountability.[102] In this manner, the SPF enables regulatory protections to

[88] Australian Government Treasury, 'Scams – Mandatory Industry Codes (Consultation paper)' (November 2023) 4 <https://treasury.gov.au/sites/default/files/2023-11/c2023-464732-cp.pdf> accessed 1 September 2025.
[89] ibid 6.
[90] ibid 4.
[91] ibid 6 (emphasis removed).
[92] 'Action on Scams, Spam and Telemarketing: October to December 2024' (*Australian Communications and Media Authority*) <https://www.acma.gov.au/publications/2025-02/report/action-scams-spam-and-telemarketing-october-december-2024> accessed 1 September 2025.
[93] Australian Government Treasury, 'Consultation paper' (n 88) 12.
[94] 'Online Investment Trading Scams Top ASIC's Website Takedown Action' (*ASIC*, 19 August 2024) <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-180mr-online-investment-trading-scams-top-asic-s-website-takedown-action/> accessed 1 September 2025.
[95] Scams Prevention Framework Bill (n 83).
[96] Revised Explanatory Memorandum to the Scams Prevention Framework Bill 2024 (Cth) 8.
[97] ibid 3.
[98] ibid 8.
[99] ibid 8.
[100] ibid 5.
[101] ibid.
[102] ibid 9.

adapt alongside the fast-paced, fluid nature of financial crime, with its coverage evolving synchronously with the emergence of new fraud typologies.[103]

Beyond its operational tools, Australia's framework embodies a more progressive theory of accountability. Its comparative 'progressiveness' is primarily substantiated by its preventative orientation: rather than treating fraud as an inevitable harm to be remedied after the fact, the SPF embeds precautionary obligations into law, mandating the collective performance of shared duties across the ecosystem, and prioritising the early disruption of fraud over post hoc remediation. A second dimension of progressiveness is reflected in its redistribution of responsibility, whereby the focus is shifted away from fraud victims, asking not whether the consumer exhibited sufficient caution, but rather whether all firms within the ecosystem met established preventative standards.[104] This stands in sharp contrast to the UK's approach, which continues to invoke consumer responsibility, even in the face of complex, socially engineered crimes that knowingly exploit systemic vulnerabilities.[105] While there are legitimate constraints on replicating such a model in the UK, ranging from legal differences in data protection to questions of political will, the comparative insight remains invaluable.[106] The Australian framework exemplifies what a genuinely proactive, multisectoral response to APP fraud can achieve and offers a blueprint for embedding preventative obligations into the UK's financial crime strategy. If the overarching aim is to protect consumers in an evolving economy shaped by cross-sector vulnerabilities, the law must evolve beyond piecemeal and institutionally isolated deferral mechanisms and towards an integrated, intelligence-driven model of fraud prevention.

In the interests of a balanced analysis, it should be underscored that the Australian model is not without its own comparative deficiencies. Most notably, the SPF does not impose an overarching legal requirement to reimburse fraud victims.[107] Rather, the SPF establishes a comparatively narrow compensatory avenue, whereby consumers may seek compensation where regulated entities have not satisfied their obligations under the SPF and the consumer has consequently 'suffered a loss'.[108] To this end, regulated entities are required to maintain an 'internal dispute resolution' ('IDR') mechanism that is both 'accessible' and 'transparent', so as to allow businesses to resolve consumer complaints in a 'timely' and 'efficient' manner.[109] Where an entity finds that it did not meet its prescribed obligations, claims will either (i) be resolved and compensated at the IDR stage;[110] or (ii) where said entity does not satisfactorily resolve the preliminary complaint, be referred to an independent 'external dispute resolution' service, at no added cost to the consumer;[111] or (iii) be resolved in court, with losses recovered

[103] ibid 5.
[104] George Iddenden, 'Crafting Security: Australia's Strategic Approach to Combatting Fraud' (*The Payments Association*, 7 June 2024) <https://thepaymentsassociation.org/article/crafting-security-australias-strategic-approach-to-combatting-fraud/> accessed 31 August 2025.
[105] Letter from Helen Charlton (15 September 2023) 2–4 <https://www.fca.org.uk/panels/consumer-panel/publication/20230912_final_fscp_response_-_psr_app_scam_mandatory_reimbursement_regime.pdf> accessed 31 August 2025.
[106] The Payments Association, 'The Impact of APP Fraud' (n 11) 32.
[107] Claudine Salameh and Tamsyn Sharpe, 'Combatting Scams in Australia and the United Kingdom' (*K&L GATES*, 19 February 2025) <https://www.klgates.com/Combatting-Scams-in-Australia-and-the-United-Kingdom-2-19-2025> accessed 31 August 2025.
[108] Australian Government Treasury, 'Protecting Australians from Scams' (n 87) 7.
[109] Revised Explanatory Memorandum (n 96) 55.
[110] ibid 58.
[111] ibid 170.

by way of damages.[112] By contrast, the UK's APPRS presents a more comprehensive, consumer-facing fraud reimbursement model, wherein consumers are automatically entitled to compensation upon victimisation and the evidentiary burden rests, not on the consumer to demonstrate institutional non-compliance, but on the regulated entity to demonstrate the applicability of specified exceptions. Accordingly, this article does not purport to cast the Australian model as a structural prototype. Rather, it serves to highlight the critical significance of a preventative regulatory posture, offering lessons that might meaningfully inform the UK's future policy trajectory.[113]

Finally, it is also instructive to consider how UK law has already begun to experiment with prevention-based liability frameworks in adjacent contexts. The 'failure to prevent fraud' offence ('FTPFO') under the ECCTA 2023[114] may be taken to illustrate how UK law is becoming increasingly receptive to the imposition of corporate liability for failure to prevent fraud. To be clear, the FTPFO does not directly target APP fraud, as the offences established by the ECCTA 2023 pursue a distinct legislative purpose. The FTPFO seeks to target organisations where persons 'associated with the body' commit a fraud offence with the intention of benefiting either the organisation itself[115] or persons to whom the organisation provides its services.[116] Significantly, the FTPFO's liability framework is not predicated upon actual or constructive knowledge by senior management: the offence applies even in the absence of board-level awareness.[117] Instead, the inquiry hinges upon whether the organisation had in place 'such prevention procedures as it was reasonable in all the circumstances to expect the body to have',[118] qualified only by section 199(4)(b), which excludes liability where no such procedures could reasonably have been expected.[119] Notably, the FTPFO is also cross-sectoral in scope, operating as an economy-wide fraud management tool, rather than an industry-specific intervention mechanism. Thus, while the ECCTA 2023 does not specifically capture APP fraud, it is theoretically informative. The FTPFO exemplifies how Parliament has already embraced a model of liability grounded not in active wrongdoing, but in a corporate duty to prevent fraud, measured against the benchmark of 'reasonable procedures'.[120] In this light, APP fraud presents itself as a natural candidate for a comparable prevention-oriented duty, one that would serve the policy objective of compensating fraud victims while recognising the injustice of imposing disproportionate burdens on financial institutions for fraud facilitated by other corporate actors.

[112] ibid 102.
[113] It may be noted that industry calls for such reforms have already long been underway. For further detail, see The Payments Association, 'Written Evidence Submitted by The Payments Association' (October 2023) <https://committees.parliament.uk/writtenevidence/125940/pdf/> accessed 1 September 2025.
[114] The 'failure to prevent fraud' offence is set out in sections 199–206 and schedule 13 of the Economic Crime and Corporate Transparency Act 2023 ('ECCTA 2023').
[115] ibid s 199(1)(a).
[116] ibid s 199(1)(b).
[117] Home Office, 'Economic Crime and Corporate Transparency Act 2023: Guidance to Organisations on the Offence of Failure to Prevent Fraud' (November 2024) 5 <https://assets.publishing.service.gov.uk/media/67f8ef1845705eb1a1513f35/Failure+to+Prevent+Fraud+Guidance+-+English+Language+v1.6.pdf> accessed 30 August 2025.
[118] ECCTA 2023, s 199(4)(a).
[119] ibid s 199(4)(b).
[120] For further detail on the definition and scope of 'reasonableness' in the context of prevention procedures under the FTPFO, see UK Finance, 'Failure to Prevent Fraud: Guidance for the Financial Services Sector' (February 2025) 15, 19–25 <https://www.ukfinance.org.uk/system/files/2025-02/UK%20Finance%20Failure%20to%20Prevent%20Fraud%20industry%20guidance.pdf> accessed 31 August 2025.

VI. Conclusion

In assessing the legal protection afforded to victims of APP scams in the UK, this article has demonstrated that, while the APPRS marks a commendable step forward when contrasted with the historical status quo, it remains a framework structured by omission. From arbitrary thresholds and institutional exclusions to under-defined vulnerability guidance, the APPRS frequently privileges institutional efficiency over the lived realities of fraud victims. Moreover, while recent amendments have introduced preventative measures, the broader framework continues to fall short of constituting a truly proactive, integrated fraud prevention regime. Nonetheless, the foregoing comparative analysis exhibits the availability of alternative models that reallocate liability from fraud victims to institutions that are better equipped to manage systemic risks. Australia's WOE approach and the UK's evolving willingness to engage with prevention-based liability frameworks under the ECCTA 2023 reflect a shared trajectory in this regard. The challenge for UK policymakers is therefore not conceptual, but practical. The legislative task ahead is to move beyond isolated, industry-specific interventions and towards an integrated solution in which strategic prevention, collective accountability, and consumer redress form part of a single regulatory framework.