Journal of Financial Regulation, 2024, **00**, 1–20
https://doi.org/10.1093/jfr/fjae006
Article

OXFORD

'Authorized Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like?

Jo Braithwaite*

ABSTRACT

Authorized Push Payment (APP) fraud occurs where bank customers are tricked into transferring money from their account. As this article shows, this type of fraud is a growing threat, catalysed by the rise of remote banking. However, long-standing legal and regulatory rules leave most victims without a route to redress, as recently confirmed by the UK Supreme Court's 2023 decision in *Philipp v Barclays*. Through this lens, the article examines a new and 'world first' UK regulatory response, which includes a mandatory reimbursement scheme for APP fraud victims in certain circumstances. The article finds that the UK's new loss allocation scheme is valuable, but also that its specific coverage is problematic given the broad nature of this threat. Overall, the article argues that the priority for UK regulators should be to develop a more 'joined-up' response to APP fraud, and it offers generally applicable insights into effective regulatory responses to this evolving threat.

KEYWORDS: APP fraud, banks, banking, Quincecare, payments, payment infrastructure

I. INTRODUCTION

Authorized Push Payment (APP) fraud is a label for a range of scams whereby a bank customer is tricked into transferring money from their account, thinking that they are engaged in a legitimate transaction. UK financial regulators, including the Payment Systems Regulator (PSR) and Financial Conduct Authority (FCA), confirm that APP fraud is a fast-growing problem,[1] closely linked to the increased use of online banking and social media. The latest report from

* Jo Braithwaite, Professor of Law, London School of Economics Law School, LSE, Houghton Street, London, UK, WC2A 2AE. Email: j.p.braithwaite@lse.ac.uk.

[1] The author would like to thank the organizers and participants at the UCL Commercial Contracts conference held in May 2023 and the LSE Law School Private Law Hub for the opportunities to present an earlier version of this article, as well as the anonymous referees for their helpful comments. Any errors are the author's. This article states the law as at November 2023. This is, however, a fast-developing area of law and regulation, and during the publication process there was opportunity to make reference in section V.2 to some of the more recent scholarship on the July 2023 Supreme Court decision in *Philipp v Barclays Bank UK plc* [2023] UKSC 25, for which the author thanks the editors. According to the PSR, fraud is the most common crime in the UK and 'APP scams are rising quickly. They have now overtaken card fraud to become the largest type of payment fraud, both in the number of scams and the value of losses.' PSR, 'Consultation Paper: Authorised Push Payment (APP) scams: Requiring Reimbursement' (CP22/4) (September 2022) [1.3] ('PSR Consultation Paper'). The FCA reports that the 'volume and variety of fraudulent activity in the UK is increasing, with APP fraud increasing year-on-year'. FCA, 'Authorised Push Payment Fraud TechSprint' (September 2022) <https://www.fca.org.uk/events/authorised-push-payment-fraud-techsprint> (all websites last accessed 10 June 2024).

Received 15 November 2023; **revised** 4 June 2024; **accepted** 5 June 2024

UK Finance underlines the scale of the problem, setting out that, in 2022, £485.2 million was lost in 207,372 incidents of APP fraud.[2] Referencing the level of banking-related fraud in the UK, and in light of the sophistication and technological know-how demonstrated by fraudsters, UK Finance concludes that 'it must be considered a national security threat'.[3] Other jurisdictions have reported similar developments; for example, in the US, levels of APP fraud relating to crypto-scams soared during the Covid-19 pandemic,[4] while in Singapore, recent large-scale APP frauds included an 'aggressive and highly co-ordinated' scam which targeted customers of OCBC Bank.[5]

The starting point for the analysis in this article is the nature of the contemporary threat of APP fraud, which, as section II shows, exploits social media and remote banking in sophisticated and opportunistic ways, and transcends traditional categories of vulnerability. As the article goes on to explain in section III, the evolution of APP fraud has highlighted the lacuna in legal protections for victims of fraud involving authorized bank transfers, which stands in contrast with the position for victims of fraud where money is taken from an account (ie, through unauthorized transfers).

Having explored the default legal position, the discussion proceeds to evaluate the UK's ongoing regulatory responses to APP fraud, including current measures and an incoming, 'world first',[6] mandatory reimbursement scheme being implemented pursuant to s 72 of the Financial Services and Markets Act 2023 (FSMA). Taking account of the growing and wide-ranging threat of APP fraud, the article focuses on the coverage of the UK's regulatory responses to date. On this basis, the article finds that the UK's current and incoming schemes are valuable because they provide new protections coupled with a loss allocation regime for victims of certain frauds in scope. However, the article also establishes that the piecemeal nature of current and incoming protections leaves certain categories of victims of APP fraud out of bounds, potentially based on factors that may be arbitrary as regards victims, such as which payment infrastructure or currency was involved in a fraud. Furthermore, as section V shows, after the landmark 2023 Supreme Court decision *Philipp v Barclays*,[7] private law is now poorly placed to act as a 'backstop' for fraud victims whose cases are not covered by regulatory schemes. Drawing these findings together, the article concludes that gaps in the coverage of redress schemes are likely to become an increasingly serious problem, as both the payments sector and the threat of APP fraud continue to evolve.

II. APP FRAUD IN CONTEXT

A widely adopted taxonomy presents eight types of APP scams, grouped under two headings of 'Malicious Payee' and 'Malicious Redirection'.[8] This taxonomy is valuable, especially in terms of awareness-raising, but, in the context of analysing an overall legal and regulatory response, there is a risk of fragmenting the discussion of issues that should be addressed with consistency.

[2] UK Finance, *Annual Fraud Report: The definitive overview of payment industry fraud in 2022* (10 May 2023) 47 ('UK Finance 2023 Report'). UK Finance is an industry body representing some 300 banking and finance firms providing services in the UK, see <https://www.ukfinance.org.uk/membership/find-member>.

[3] UK Finance, *2022 Half Year Fraud Update* (13 October 2022) 3 ('UK Finance 2022 Update').

[4] See further section II.

[5] OCBC, 'OCBC Bank has been making goodwill payments to victims of the recent SMS phishing scam since 8 January 2022' (17 January 2022) <https://www.ocbc.com/group/media/release/2021/goodwill-payouts-for-scam-victims.page>.

[6] PSR, 'Policy Statement: Fighting authorised push payment fraud: a new requirement. Response to September 2022 consultation (CP22/4)' (PS23/3) (June 2023) 3 ('PSR June 2023 Policy Statement').

[7] *Philipp v Barclays Bank UK plc* [2023] UKSC 25.

[8] The usual taxonomy is: (1) Malicious Payee, comprising purchase scams, investment scams, romance scams and advance fee scams; and (2) Malicious Redirection, comprising invoice and mandate scams, CEO fraud, impersonation: police/bank staff and impersonation: other. See, eg, UK Finance 2023 Report (n 2) 52; PSR, 'APP scams' <https://www.psr.org.uk/our-work/app-scams/>.

For this purpose, it is therefore more constructive to begin by locating this type of fraudulent activity in its broader social and economic context.

1. Social engineering

One clear theme that emerges from reported cases,[9] as well as police, industry, and bank guidance,[10] is the extent to which APP frauds of diverse types involve so-called 'social engineering' often enabled by various forms of technology. Tellingly, numerous decisions by the United Kingdom's Financial Ombudsman Service (FOS),[11] describe the state of mind of victims in identical terms, namely, that they are made to act 'under the spell' of the fraudsters.[12] This was also a feature of the leading APP fraud case to come to the UK courts to date.[13] In this case, a month or so of interaction between fraudsters and a married couple ultimately persuaded the couple to transfer away the bulk of their life savings, leading the judge to conclude that:

> There is no scope on this application for proceeding otherwise than on the basis that the Philipps were 'completely **under the spell of the fraudster**' . . . which, subject to allowance for any relatively modest cash payments they may have received from [the fraudster], has presently cost them £700,000.[14]

This kind of social engineering means that even sophisticated anti-fraud checks by payment services providers can be futile. For example, reported decisions record victims being told by fraudsters exactly how to respond to banks' anti-fraud questions, therefore bypassing checks built into the 'payment journey'.[15] Consequently, while robust, co-ordinated anti-fraud processes, like the 'digital security controls' and 'good cyber hygiene' currently being promoted by

[9] Including consumer tribunal decisions and court cases. For the former, published with anonymity as to claimants, see the UK 'Financial Ombudsman Service' website <https://www.financial-ombudsman.org.uk/decisions-case-studies/ombudsman-decisions>. For further detail about the jurisdiction of the FOS, see nn 11 and 12.

[10] For instance, UK Finance 2023 Report (n 2) 7; Action Fraud (run by the City of London Police and National Fraud Intelligence Bureau), in its guidance about types of fraud, covers romance scams which 'involve people being duped into sending money to criminals who go to great lengths to gain their trust and convince them that they are in a genuine relationship. They use language to manipulate, persuade and exploit . . . ' Action Fraud, 'Romance scams' <https://www.actionfraud.police.uk/a-z-of-fraud/romance-scams>; the FOS also warns that 'As well as technology, scammers will try to manipulate or exploit situations to build trust, or create a sense of urgency or panic, to get you to reveal information to them over the phone and sometimes even face to face.' See FOS, 'Staying safe from scams and what to do if you're caught out' <https://www.financial-ombudsman.org.uk/data-insight/insight/avoiding-fraud-and-scams>. By way of example of banks' warnings, HSBC posts regular updates about the 'latest types of scams' which routinely include elements of social engineering by fraudsters, eg posing as police, tax authorities or government employees, or using deepfake technology; see HSBC, 'Latest scam warnings' <https://www.hsbc.co.uk/help/security-centre/latest-scam-warnings/>.

[11] The FCA Handbook sets out how complaints are to be dealt with by respondents in scope and how complaints that are not resolved internally may be considered by the FOS. See FCA Handbook, 'Dispute resolution: Complaints, "DISP"'. From 31 January 2019, victims of alleged APP fraud, where they are eligible complainants, fall within these provisions. See FCA, 'Policy Statement: Authorised push payment fraud—extending the jurisdiction of the Financial Ombudsman Service' (PS18/22) (December 2018). FOS award limits were raised from 1 April 2022 to £375,000 for complaints referred to the FOS on or after that date, regarding acts or omissions on or after 1 April 2019. See FOS, 'Increase to our award limits' (FOS, 18 March 2022) <https://www.financial-ombudsman.org.uk/news-events/increase-award-limits>.

[12] Including FOS Decision DRN-2861101 (7 June 2021) 3, in relation to a romance scam. The following FOS decisions are further examples which consider whether the banks involved could have 'broken the spell' affecting the victim: relating a crypto-asset scam, see FOS Decision DRN-3759935 (15 December 2022); FOS Decision DRN-3712816 (16 November 2022), in which a romance scam involved a cryptocurrency scam; and relating to bank/police impersonation scams, see FOS Decision DRN-2555849 (19 March 2021).

[13] *Philipp v Barclays Bank UK plc* [2021] EWHC 10 (Comm) [27]–[71]. See further section V.

[14] *Philipp v Barclays Bank UK plc* [2021] EWHC 10 (Comm) [71] (Judge Russen QC, sitting as a High Court judge), referring to the witness statement of the claimant's solicitors, in turn, picking up the language of the bank's solicitor in her witness statement. Emphasis added.

[15] For example, FOS Decision DRN-3761062 (5 December 2022) 1, records that the customer was instructed by the fraudster to respond to the bank's fraud check by stating that 'she was acting alone, and the payment was authorised', which she did.

the Association of Banks in Singapore,[16] are clearly part of a comprehensive response to APP fraud, it remains inevitable that the question of when to reimburse victims will continue to arise.

2. Remote banking

New opportunities to undertake the kind of social engineering described above have been created in the course of systemic changes underway in the banking sector. The most relevant developments for this purpose are the greater take-up of remote (ie telephone, mobile phone app, and online) banking, now used by some 86 per cent of all adults in the UK,[17] and of online investment platforms, alongside associated changes in the payments landscape. The last includes the steady decline in the use of cash,[18] and what UK Finance predicts will be 'ongoing growth in Faster Payments and other remote banking payments', currently at some 3.6 billion payments a year and 'growing strongly' in popularity.[19]

There are, of course, important positive outcomes from these developments. These include customer convenience, speed of payments, greater competition resulting from new online-only banks and other new entrants to the sector,[20] and the diversification of payment service providers associated with the introduction of Open Banking.[21] The expanding opportunities for APP fraud on an unprecedented scale are, however, a toxic side-effect. UK Finance reports that in the second half of 2022, the vast majority (78 per cent) of APP fraud cases by number originated online,[22] while the PSR notes that 'Criminals are getting more creative and sophisticated each day'.[23] Consequently, any analysis of the legal and regulatory response to APP fraud must also take account of the rapidly changing banking and payments landscape, and the proven capacity of fraudsters to exploit new opportunities in sophisticated ways.

3. Covid-19

Systemic changes in the banking and finance sector, which are creating new opportunities for APP fraud as a side-effect, have been further catalysed by measures associated with the Covid-19 pandemic. The pandemic period saw increased use of mobile and online banking, coupled with extensive social isolation and the greater use of social media,[24] and it is now apparent that banking fraud also reached 'record highs' during the pandemic.[25]

16 The Association of Banks in Singapore, 'Industry Guidelines: Standing Committee on Fraud' <https://www.abs.org.sg/industry-guidelines/fraud#:~:text=The%20ABS%20Standing%20Committee%20on,rising%20occurrence%20of%20digital%20scams>.

17 UK Finance, 'UK Payment Markets Summary 2022' (August 2022) 5 ('UK Finance Summary').

18 UK Finance reports that, since 2017, the use of cash has been declining by some 15 per cent each year, with an acceleration of this decline in 2020, and a slowing of the rate of decline in 2021. Nonetheless, in 2021 1.1 million people in the UK 'mainly used cash' in their day-to-day lives. UK Finance Summary (n 17) 2, 4.

19 UK Finance Summary (n 17) 5 and 8, including the prediction that payment volumes over the Faster Payment System will increase to 5.7 billion by 2031. The FPS infrastructure is explained further in section IV.

20 The need for more effective competition in the supply of retail banking services to personal current account customers and small and medium-sized enterprises was identified by the 2014–16 investigation by the Competition and Markets Authority (CMA), *Retail banking market investigation: Final report* (9 August 2016), to which there have been diverse and ongoing responses. Note also the post-global financial crisis introduction of the promotion of competition into the operational objectives of the FCA (Financial Services and Markets Act 2000 s 1E) and PSR (Financial Services (Banking Reform) Act 2013 s 50).

21 Open Banking allows consumers and small and medium-sized enterprises (SMEs) to share their bank data with third parties providing apps, services, and access to payments, based upon open application programming interface (API) technology, with the aim of increasing efficiency for the customer. It is supported by provisions in the Payment Services Regulations 2017 SI 2017/752 ('PSRegs').

22 UK Finance 2023 Report (n 2) 49. Note that this accounted for 36 per cent of reported APP fraud by volume, leading this report to conclude that online scams tend to involve lower-value cases than other types of APP fraud.

23 PSR Consultation Paper (n 1) [1.4].

24 The greater risk of economic fraud during the pandemic was highlighted contemporaneously, eg in a warning from 26 March 2020 from the National Crime Agency (NCA): NCA, 'Beware fraud and scams during Covid-19 pandemic fraud' (sic) (NCA, National Economic Crime Centre and City of London Police) <https://www.nationalcrimeagency.gov.uk/news/fraud-scams-covid19?highlight=WyJjb3ZpZC0xOSJd>.

25 UK Finance 2022 Update (n 3) 2.

One indication of how these various factors have coalesced is that regulators report a dramatic jump in APP scams relating to crypto-assets during the pandemic. For example, in the US, losses from cryptocurrency fraud reported to Federal Trade Commission soared from $130m in 2020 to $680m in 2021, up 60 times since 2018, while in the period January 2021–March 2022, $575m of reported cryptocurrency losses were the result of investment scams, described by the US regulator as the result of 'a perfect storm: false promises of easy money paired with people's limited understanding and experience'.[26] Amongst myriad harms, therefore, the Covid-19 pandemic catalysed the problem of APP fraud and left many bank customers more vulnerable, thereby heightening the urgency of a regulatory response.

4. Vulnerability

Looking at APP fraud in its wider social and economic context therefore shows that the threat is not confined to a specific type of scenario, victim, payment method, or infrastructure; if it were, it would enable a regulatory response to be precisely targeted. Instead, the perpetrators of APP fraud skilfully exploit new opportunities to 'socially engineer' diverse types of victims, harness cutting-edge technology, and manipulate anti-fraud checks. Consequently, in the post-pandemic economy, vulnerability to APP fraud has transcended traditional paradigms of vulnerability relating, for example, to age or status. As sensibly reflected in one of the UK's schemes covering APP fraud, explored further in section IV, vulnerability to this kind of fraud is therefore best thought of as universal, meaning that any person, or any legal entity that individuals are authorized to act for, is potentially a victim.[27] Consequently, an effective legal and regulatory response to APP fraud must take into account the scale and universality of the threat, alongside the proven capacity of fraudsters to exploit new opportunities as they arise.

III. LEGAL FUNDAMENTALS

The core relationship between bank and account-holder is one of contract[28] (today, principally made up of express terms),[29] while regulation layers around this core contract, as do soft law codes and industry best practices.[30]

When a customer makes payments from their bank account, both contractual terms and regulations therefore apply. Standard contracts governing personal current accounts include extensive express terms about 'Making payments from your account'[31] covering the methods by which a customer may authorize a payment from their account and the requirements of such instructions.[32] In practice, these express terms operate in conjunction with various regulatory provisions. In the EU and UK, the most significant provisions for this purpose derive from the Payment Services Directive 2015,[33] implemented in the UK through the Payment Services Regulations 2017 SI 2017/752 ('PSRegs'), which apply to a broad range of transfers. Certain

[26] Emma Fletcher, 'Reports show scammers cashing in on crypto craze' (Federal Trade Commission, *Consumer Protection Data Spotlight*, 3 June 2022) <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze>. See footnote 1 in this FTC document for details of fraud data reported to the FTC.

[27] See the discussion of the CRM Code in section IV.1.

[28] Across common and civil law: see Danny Busch and Cees Van Dam (eds), *A Bank's Duty of Care* (Bloomsbury 2017), see in particular, Part V: Comparative Conclusions.

[29] See, eg, the 56 pages of 'Barclays and you: Terms and conditions for personal customers' (November 2020) <https://www.barclays.co.uk/important-information/personal-terms-conditions/>.

[30] For a comprehensive review of the different legal and regulatory elements of this relationship, see Ross Cranston and others, *Principles of Banking Law* (3ed edn, OUP 2017) ch 7.

[31] For, eg, Barclays, Terms and conditions (n 29) 28–34.

[32] Barclays, Terms and conditions (n 29) 29.

[33] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market [2015] OJ L 337/35.

provisions of the PSRegs may be excluded, but only by more sophisticated customers (and not by consumers).[34]

Authorized payment transfers are defined in the PSRegs as those where the payer has given consent to the execution of the payment transaction, or the series of transactions which it is part, 'in the form, and in accordance with the procedure, agreed between the payer and its payment service provider . . . '.[35] Banks have a strict duty to follow duly authorized payment instructions, and act as their customers' agent as they do so.[36] Because *unauthorized* transfers are made without the bank having valid customer instructions, the default rule under both common law[37] and the PSRegs[38] provides for reimbursement of the customer (no later than the end of the business day following the day on which the bank becomes aware of the unauthorized transaction, if the PSRegs applies).[39] By definition, however, authorized payments fall outside the rules governing reimbursement for unauthorized transfers; victims of frauds involving authorized payments, and their banks, have therefore traditionally faced a legal and regulatory lacuna.

Until very recently, in fact, there was even provision in regulation 90 of the PSRegs stating that banks would not face liability if the customer used an incorrect payee account number or sort code.[40] Section 72(11) of the FSMA, however, qualifies regulation 90 so that payment service provider liability is now possible where the payment order is 'executed subsequent to fraud or dishonesty' but only where such liability arises under one of the listed statutory routes (for example, under a direction of the PSR addressed to all or specific regulated persons).[41] Even once these provisions come into force, the PSRegs themselves will not provide a concrete regime for the allocation of losses arising from APP fraud, as it does for unauthorized payments, but the change creates space for such schemes, as discussed further in section IV.

In the absence of any legal route to redress, victims of push fraud sometimes receive a 'goodwill' reimbursement from their bank.[42] Given that the vast majority of APP fraud cases by number is reported by individuals,[43] and can involve sums that are relatively small from the bank's perspective, the practical importance of this informal outcome should not be underestimated.[44] However, failing an accepted offer of a goodwill payment, the fate of

[34] PSRegs reg 63(5) provides that payment service providers may only agree to exclude key parts of the provisions relating to unauthorized and defective/non-execution of payments with parties who are not consumers, micro-enterprises, or charities.

[35] PSRegs reg 67.

[36] As discussed in *Philipp v Barclays Bank UK plc* [2023] UKSC 25 [28]–[30].

[37] In this scenario, the bank is acting without the customer's authority and the transaction is therefore not binding on the customer, subject to certain duties on the customer such as the duty to provide instructions in a way that is clear and unambiguous following the House of Lords' decision in *London Joint Stock Bank Ltd v MacMillan* [1918] AC 777. On unauthorized transfers under common law see Cranston and others (n 30) 199–201 and S Booysen, 'Consumer protection and the court's role in shaping the bank-customer contract' (2019) 135 LQR 437, section II.

[38] PSRegs reg 76(1).

[39] PSRegs reg 76(2).

[40] PSRegs reg 90 states: '(1) Where a payment order is executed in accordance with the unique identifier, the payment order is deemed to have been correctly executed by each payment service provider involved in executing the payment order with respect to the payee specified by the unique identifier. (2) Where the unique identifier provided by the payment service user is incorrect, the payment service provider is not liable under regulation 91 or 92 for non-execution or defective execution of the payment transaction . . . '

[41] Financial Services and Markets Act 2023 (FSMA) s 72(11) which received Royal Assent on 23 June 2023, amends the PSRegs to add a new reg 90(6) to this effect. See further section IV.

[42] The importance of goodwill payments in this context is reflected in the CRM Code, (discussed in section IV), Overarching Provision, OP2: 'Nothing in this Code should prevent any Firm, whether UK-based or not, exercising its discretion to provide ex gratia payments to a Customer should it decide to do so.' LSB, 'Contingent Reimbursement Model Code for Authorised Push Payment Scams' (8 February 2023) (CRM Code). Note also the FOS route for complaints against banks, discussed in nn 11 and 12, and in the accompanying text.

[43] Of 207,372 incidents of APP fraud in 2022, 200,643 involved 'personal' accounts and the rest 'non-personal' or business accounts: UK Finance 2023 Report (n 2) 47.

[44] See, eg, the goodwill payments made by OCBC bank in Singapore, following a sophisticated SMS phishing scam which targeted its customers: OCBC Bank (n 5).

those who been scammed by an APP fraud depends on whether any legal or regulatory rules mitigate or qualify the default position in law, and the UK's current and incoming measures are considered next.

IV. UK REGULATORY RESPONSES

Section III explained that, as a matter of law, bank customers would normally bear the losses from so-called 'push' frauds. Meanwhile, as section II explored, the nature of APP fraud has evolved so that it now poses a universal risk, and data indicate that such frauds are proliferating. As such, though goodwill payments from banks have been known in some cases, pressure has grown for banks and their regulators to revisit the traditional legal treatment of push fraud and, specifically, to address loss allocation in a more formal way.

The UK's regulatory response to APP fraud was kick-started in September 2016, by a 'super-complaint' filed by the consumer association 'Which?'.[45] Many reports, surveys, and consultations have followed.[46] As this section of the article shows, regulatory schemes aimed at tackling APP fraud, and providing for losses to be borne by payment service providers in certain circumstances, have now emerged. Furthermore, while implementation has been described by the House of Commons Treasury Committee as 'painfully slow',[47] a new scheme of mandatory reimbursement for certain types of APP fraud is due to come into force in October 2024. This UK mandatory scheme will be a 'world first',[48] and in this sense it is of wider relevance, given the scale of the threat of APP fraud worldwide. As the UK regulator points out, 'The UK is the first country in the world to implement consistent standards to reimburse victims of APP fraud, and other jurisdictions are watching closely in considering their own approaches'.[49]

This section of the article analyses the relevant regulatory schemes that have been implemented in the UK to date, addressing first the schemes which have been in place since around 2019, and then turning to the forthcoming mandatory reimbursement scheme. In light of the discussion in section II, which established the universal and shifting risk of APP fraud, the analysis here focuses principally on the themes of scope and coverage. The discussion evaluates the specific regulatory schemes implemented or being implemented in the UK so far, however, it also concludes that that the underlying risks associated with this kind of bank fraud require a more co-ordinated approach across the payments landscape. Ultimately, this conclusion also helps to explain why certain cases involving APP fraud have been brought using private law, the implications of which are considered in section V.

1. Valuable but limited: CoP and the CRM code

Prior to the statutory implementation of a new mandatory scheme for reimbursement, the regulatory response to APP fraud in the UK included two notable initiatives, which introduced valuable improvements but failed to reach millions of customers because of important limitations.

[45] Which? Super-complaint, 'Consumer safeguards in the market for push payments' (23 September 2016).

[46] For example, the PSR observes that 'We have carried out a significant amount of work to prevent APP scams since 2016.' PSR, 'APP Scams' <https://www.psr.org.uk/our-work/app-scams/>. A selection of work by other organizations active in this area since the Which? Super-complaint is referenced in section II, including work by the NCA, Action Fraud, FOS, and UK Finance, while the work of Pay.UK and the Lending Standards Board is discussed later in this section.

[47] House of Commons Treasury Committee, *Scam Reimbursement: Pushing for a better resolution* (Thirteenth Report of Session 2022–23, HC 939, 6 February 2023), para 25.

[48] PSR June 2023 Policy Statement (n 6) 3. The October 2024 start date is confirmed on the PSR website, see <https://www.psr.org.uk/our-work/app-scams/>.

[49] PSR June 2023 Policy Statement (n 6) [1.20].

The first is the 'Confirmation of Payee' (CoP) protocol.[50] This protocol is designed and operated by the retail interbank payment system operator, Pay.UK,[51] and applies when a payment instruction in its scope involves setting up a new payee. It will be unaffected by the introduction of the new mandatory reimbursement scheme. CoP identifies the name attached to the account with the numeric details provided by the payer and checks this name against the payee name provided by the payer, reporting if there is a match, partial match, no match, or if the service is not available. Absent CoP, the payee's name is ignored for these purposes. The protocol can be effective in identifying 'redirection' scams and helps payers pick up mistakes in entering data, but it does not, of course, help in cases where a fraudster has provided a matching account name and numeric details.[52]

The PSR required members of the UK's six largest banking groups to offer CoP by the end of March 2020,[53] with other entities encouraged to do so on a voluntary basis, but, according to Which?, 'millions of customers' still do not have the benefit of CoP.[54] In October 2022, the PSR directed a further 400 financial firms to provide CoP, with deadlines of end-October 2023 or end-October 2024, depending on the type of firm.[55] As at the time of this announcement, the PSR reported that 59 financial organizations offered CoP. The problem of some firms' slow take-up of this significant improvement for customers has been compounded by a lack of transparency: it is apparently not possible to find a list of those institutions that have adopted CoP and, instead, the regulator advises customers to check with each account-provider direct.[56]

The implementation of the first UK initiative designed to reimburse certain victims of APP scams has followed a similar pattern as seen with CoP. The Contingent Reimbursement Model Code ('CRM Code') was set up in May 2019[57] and administered by the Lending Standards Board (LSB), which describes itself as the 'primary self-regulatory body for the banking and lending industry'.[58] The CRM Code is extensive and comprises several different parts, opening with two 'Overarching Provisions'. As 'OP1' makes clear, the Code seeks to reduce APP scams by strengthening firms' fraud prevention and detection measures as well as providing a regime for customer reimbursement for APP scams in scope.[59] The CRM Code's reimbursement regime is the focus for the purposes of this article and, as will be seen, this provides a valuable, PSRegs-like scheme for victims of fraud in scope, therefore partly addressing the lacuna noted in section III. However, even where a payment services provider has elected to sign up, the Code is limited to certain types of fraud victims only, covering payers who are consumers, micro-enterprises,

[50] Pay.UK, 'Confirmation of Payee', explaining that this service is 'an account name-checking service designed to help reduce misdirected payments and provide greater assurance . . . for UK domestic payments' and reporting that 'more than 1.9m checks' are completed every day <https://www.wearepay.uk/what-we-do/overlay-services/confirmation-of-payee/>.

[51] See further section IV.2.

[52] Pay.UK, 'Confirmation of Payee: FAQs: Who currently offers Confirmation of Payee?' <https://www.wearepay.uk/what-we-do/overlay-services/confirmation-of-payee/faqs/>.

[53] The PSR's Specific Direction was given to Bank of Scotland plc, Barclays Bank UK plc, Barclays Bank plc, HSBC Bank plc, HSBC UK Bank plc, Lloyds Bank plc, National Westminster Bank plc, Nationwide Building Society, Royal Bank of Scotland plc, Santander UK plc and Ulster Bank Limited. See PSR, Specific Direction 10 requiring the introduction of Confirmation of Payee (August 2019, varied February 2020), [3].

[54] Chiara Cavaglieri, 'Confirmation of Payee: more firms adopt security checks to reduce fraud' (Which?, 20 September 2022) <https://www.which.co.uk/news/article/confirmation-of-payee-more-firms-adopt-security-checks-to-reduce-fraud-auNMm4N4w6Mj>.

[55] PSR, 'PSR directs 400 firms to introduce the payment protection measure, Confirmation of Payee' (*PSR, Latest news*, 11 October 2022) <https://www.psr.org.uk/news-and-updates/latest-news/news/psr-directs-400-firms-to-introduce-the-payment-protection-measure-confirmation-of-payee/>. See also PSR, 'What is Confirmation of Payee?' <https://www.psr.org.uk/our-work/app-scams/frequently-asked-questions-for-consumers/>.

[56] 'We recommend contacting your provider to check if this service is offered': PSR, 'What is Confirmation of Payee?' (n 55).

[57] For background to what was then 'the New Code' and discussion of the design, see John Taylor and Tony Galica, 'A New Code to Protect Victims in the UK from Authorised Push Payments Fraud' (2020) 35 *Banking & Finance Law Review* 327.

[58] LSB, 'Who We Are' <https://www.lendingstandardsboard.org.uk/who-we-are/>. The LSB offers various Standards and Codes which financial services firms are invited to sign up to, on the basis that registering is a signal commitment to high customer standards: LSB, 'Why Register' <https://www.lendingstandardsboard.org.uk/why-register/>.

[59] CRM Code Overarching Provisions, OP1.

and charities, while the relevant parts of the PSRegs cover all types of payers, and do not allow opt-out by those categories.[60] By default, therefore, a larger company would be covered by the rules in the PSRegs, but can never be covered by the CRM Code.

The Code's reimbursement rule follows the same, customer-friendly structure as the PSRegs, by opening with a clearly drafted default rule requiring firms to reimburse customers who have suffered loss through an APP scam,[61] which is then qualified by a list of carve-outs. Carve-outs from the default rule under the two regimes also overlap, both expressly where a customer is liable for 'gross negligence',[62] and more loosely, as regards what might be thought of as customer carelessness. The CRM Code provisions, however, are broader and more detailed as to the situations that will qualify as exceptions to the default reimbursement rule, which, if they had a 'material effect' on preventing the APP scam, enable banks to 'choose not to reimburse a Customer'.[63] For example, the CRM Code 'Exceptions' include where a customer ignores their bank's 'Effective Warnings', as defined elsewhere in the Code,[64] or a negative CoP return.[65]

Thereafter, there is even greater divergence between the CRM Code and PSRegs, reflecting that the former offers not only default rules but also guidance and processes for managing claims. Unlike the PSRegs, for example, the CRM Code addresses in some detail the nature of customer vulnerability. Rightly, given the themes discussed in section II, vulnerability in this context is to be assessed on a case-by-case basis, and in light of the significant statement that 'All Customers can be vulnerable to APP scams and vulnerability is dynamic'.[66] 'Vulnerability' itself matters within the Code because in such cases, the default reimbursement rule should be applied, notwithstanding the carve-outs discussed above.[67]

The second half of the CRM Code reflects the potential for greater complexity and controversy in APP fraud cases as compared to those involving unauthorized transactions. Unlike the PSRegs, for example, the CRM Code does not provide a specific time-frame for a reimbursement. Instead, a bank must take a decision on reimbursement no later than 15 Business days (sic), or 35 in 'exceptional cases', from when customer reports the scam, and thereafter any reimbursement must only be 'without delay'.[68] This approach contrasts with the PSRegs' more specific requirement that a refund for an unauthorized transfer should take place 'as soon as practicable, and in any event, no later than the end of the business day following the day on which it becomes aware of the unauthorised transaction'.[69]

Overall, compared to the legal position otherwise facing victims of APP fraud, the CRM Code is a great improvement for cases falling within its scope, offering a valuable 'PSRegs-like' default rule for customers, as well as clarity around contextual factors and processes. Indeed, recent data seem to confirm that the Code has significantly increased reimbursement levels: it has been reported that before the 2019 introduction of the CRM Code, victim reimbursement was 19 per cent of losses by value but, in the first half of 2022, for APP fraud victims banking with an entity signed up to the Code, the rate of reimbursement increased to 60 per cent by value (with variations between different banks), while for those outside

[60] PSRegs reg 65(5).
[61] CRM Code R1: 'Subject to R2, when a Customer has been the victim of an APP scam Firms should reimburse the Customer.' Compare PSRegs reg 76(1).
[62] PSRegs reg 77(3)(b); CRM Code R2(1)(e).
[63] CRM Code R2(1).
[64] CRM Code R2(1)(a).
[65] CRM Code R2(1)(b).
[66] CRM Code R2(3).
[67] CRM Code ALL2(4).
[68] CRM Code R3(1).
[69] PSRegs reg 76(2).

the scheme, there was a lower reimbursement rate of 44 per cent by value.[70] On this basis, however, the voluntary nature of the Code has become problematic both in principle and in practice, as take-up has been uneven. Ten 'firms' (the LSB's term for bank, building society, or banking group signatories) have registered with the CRM Code as at October 2023, with some firms covering multiple brands.[71] This represents significant participation in the scheme but important gaps remain; by way of comparison, 19 'firms' have signed up to another of the codes of practice offered by the Lending Standard Board, namely the 'Standards of Lending Practice for personal customers',[72] while the Bank of England reports that as at June 2022, there were 37 settlement bank members of the payment systems Faster Payments and CHAPS, and 27 for BACS.[73]

2. Mandatory reimbursement scheme

Given the uneven take-up of the voluntary CRM Code, there has long been pressure for a more powerful regulatory approach,[74] and a mandatory reimbursement scheme for certain APP frauds has now been provided for in the FSMA, which received Royal Assent on 29 June 2023. As already noted, this development has been labelled as a 'world first' by UK regulators; however, while the mandatory scheme incorporates certain valuable features of the CRM Code, as this section explains, significant questions around coverage follow from this policy and should now be addressed.

The FSMA requires the PSR, within six months of the relevant section coming into force, to consult on and implement a 'relevant requirement for reimbursement' for payment service providers with respect to APP scam victims 'in such qualifying cases of payment orders as the Regulator considers should be eligible for reimbursement'.[75] The statutory definition of 'qualifying cases' provides that they are payments which are made 'subsequent to fraud or dishonesty' and executed over the 'Faster Payments Scheme' infrastructure only.[76]

The Faster Payment System (FPS) is one of the major UK payment infrastructures, operated by Pay.UK, supervised by the Bank of England, and regulated by the PSR. It is a 24/7 near 'real time' payment system, processing a vast majority of intra-UK internet, mobile, and telephone banking payments up to £1 million, and routinely used by individuals, charities, and businesses. In 2022, 3.4 billion transactions were processed with a value of £2.6 trillion.[77] Without question, therefore, the new mandatory reimbursement scheme will cover the vast majority of APP frauds by payment system used: the PSR reports that in 2021, FPS was used for 97 per cent of APP scam payments by number (making up 0.1 per cent of overall payment volumes on the service).[78] By

[70] House of Commons Treasury Committee, *Scam Reimbursement* (n 47) para 6 drawing upon data from LSB, UK Finance, and Which?.

[71] Barclays Bank UK PLC, Co-operative Bank plc, HSBC UK Bank plc, Lloyds Banking Group, Metro Bank plc, National Westminster Bank plc, Nationwide Building Society, Santander UK plc, Starling Bank Ltd, Virgin Money UK plc: registered banks available at LSB, 'Registered Firms' <https://www.lendingstandardsboard.org.uk/registered-firms/>.

[72] LSB, 'Registered Firms' (n 71).

[73] The Bank of England, *The Bank of England's supervision of financial market infrastructures: Annual Report 15 December 2021–16 December 2022* (2022) 39 ('Recognised payment systems and securities settlement systems').

[74] For example, Which?, 'Banks will have to repay bank transfer scam victims under new law: The Government commits to making reimbursement mandatory for scam victims, following Which? Campaign' (*Which? Online news*, 18 November 2021).

[75] FSMA s 72(1)–(10). The focus here is the reimbursement requirement being implemented by the PSR, but this is accompanied by other PSR initiatives relating to the prevention of APP fraud.

[76] FMSA s 72(2). Note that the Act refers to the 'Faster Payments **Scheme**', but following Pay.UK, either 'Faster Payment **System**' or FPS is used in this article.

[77] See Pay.UK, 'Faster Payment System' <https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/>.

[78] PSR Consultation Paper (n 1) [1.6]; the PSR's 2021 'Call for views' gave the figure of 86 per cent of APP scam losses taking place over Faster Payments and Bacs Direct Credit: PSR, 'Authorised push payment (APP) scams: Call for views' (CP21/3) (February 2021) 9.

comparison, the CHAPS payment system, which is not covered by the new scheme although it was covered by the CRM Code, is typically used for much higher value payments. Accordingly, while CHAPS accounts for 0.2 per cent of APP scams by volume, these transfers are 4 per cent of APP scams by value.[79]

As expressly anticipated in the FSMA, by the time of Royal Assent, the PSR had already run a consultation around a proposed scheme and published a follow-up policy statement and near-final version,[80] with the stated aim of the new scheme coming into force in 2024.[81] These materials confirm that the PSR's mandatory reimbursement scheme will require:[82]

- all payment services providers (including indirect participants) sending payments over FPS;
- where there is a **qualifying case** of APP fraud (defined as an authorized payment from an account controlled by a customer to an account controlled by someone else, authorized by the customer as part of an APP fraud and executed over FPS);
- to reimburse APP fraud victims who are 'consumers, micro-enterprises and charities' (defined for this purpose as 'consumers' and expressly following the definitions of these terms in the PSRegs);
- who report the fraud within 13 months (consistent with the time limit for reporting unauthorized transfers under the PSRegs);
- reimbursement to take place within five working days after being notified of the fraud unless the payment service provider 'stops the clock' for one of the permitted purposes (this allows the payment service provider time to 'gather additional information from victims to assess the claim');[83]
- with exceptions to reimbursement in the case of fraud or gross negligence by the payer, with the latter not applicable where the payer was vulnerable (but adopting the narrower definition of vulnerability from the FCA, rather than the more inclusive definition under the CRM Code, discussed above);[84]
- providing for the costs of mandatory reimbursement to be allocated between sending and receiving payment services providers, with a default 50:50 split; and
- with a maximum level of reimbursement and a £35 excess applicable to reimbursements, which are both subject to further consultation.

On this basis, the core objective and certain important features of the new PSR scheme will follow the precedent of the CRM Code but only for 'qualifying cases' made over FPS. For these 'qualifying cases', given that the scheme is mandatory, the PSR scheme will tackle the central weakness of the CRM Code, and has therefore been widely welcomed, including by consumer associations supportive of 'the high level of customer protection proposed'.[85] In terms of the practical relationship between the two regimes, the suggestion in the latest PSR policy statement

[79] PSR Consultation Paper (n 1) [4.9]. See further section IV.3.

[80] PSR Consultation Paper (n 1), along with the PSR June 2023 Policy Statement (n 6).

[81] PSR, 'PSR confirms new requirement for APP fraud reimbursement' (7 July 2023) <https://www.psr.org.uk/news-and-updates/>.

[82] Based on details of the proposed reimbursement requirement found in the PSR Consultation Paper (n 1) [1.16]–[1.22], and PSR June 2023 Policy Statement (n 6) 6–7, setting out 'ten key policies' underlying this scheme.

[83] PSR June 2023 Policy Statement (n 6) 44, Box 5.

[84] PSR Consultation Paper (n 1) [4.27]–[4.28], citing FCA, FG21/1, 'Guidance for firms on the fair treatment of vulnerable customers' (February 2021), where the FCA definition of 'vulnerable customer' is 'someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care'.

[85] See PSR, 'Policy Statement: Fighting authorised push payment fraud—Annex 3: Question-by-question feedback and response to our consultation' (PS23/3 Annex 3) (June 2023) [1.2].

is that the two schemes will not run in parallel, but that the new scheme will take over from the CRM Code.[86] This heightens the significance of the coverage of the new scheme.

Shifting from a voluntary to mandatory reimbursement scheme has, understandably, been welcomed by consumer groups but it also intensifies the rule-making challenge that Parliament has determined the PSR should be responsible for. The most obvious trade-off has been the narrower focus of the PSR scheme, focusing only on payments made through FPS infrastructure, rather than the broader coverage of the CRM Code, which also extends to payments made using CHAPS and transfers within the same bank. This key question of coverage of different payment systems considered further in the next section; however, there are other points of divergence between the PSR scheme and CRM Code which are also significant. These differences evidence the challenge of designing a workable, mandatory, customer-facing loss allocation scheme which, despite its narrower coverage, is still expected to apply to a diverse group of over 1500 direct and indirect FPS participants,[87] millions of customers, and trillions of pounds worth of transactions each year.

One point of divergence, for example, is the time for any reimbursement to be made to a fraud victim. The PSR scheme includes a fixed deadline for reimbursement (like the PSRegs regime for unauthorized payments, but unlike the CRM Code), but its 'five business day' limit has been extended from the more consumer-friendly 48-hour deadline provided in the original consultation. Meanwhile, 'stop the clock' rules in the PSR scheme mean that this deadline can quite easily be set aside by the banks, as noted above.[88] In other areas, rather than providing precise rules at this stage, the PSR has postponed decisions about details of the scheme until the post-implementation period. This strategy received a mixed reception during the recent consultation. In relation to detailed rules for interbank loss allocation, for example, the latest policy statement continues to provide that Pay.UK, post-implementation, will develop detailed 'operational guidance and processes for the reimbursement process between sending and receiving [firms]'.[89] In relation to some fundamental, customer-facing aspects of the scheme, however, this approach has had to be revisited. For example, in terms of defining the meaning of gross negligence (important in this context because it defines when a customer does not have to be reimbursed) the proposal was that no PSR guidance was to be issued with the scheme, with the standard to be revisited post-implementation.[90] However, by the time of the June 2023 Policy Statement, the PSR had agreed to develop its own guidance on this standard, to be published before the scheme comes into effect.[91] This may be challenging work within the time-frame, but it seems correct to have guidance on a point of such general importance to the customer-facing aspects of the scheme in place before implementation.

There is, in fact, relatively little in official publications to date about how the reimbursement scheme will actually run post-implementation, though it has been clear throughout the debates that the PSR supports responsibility for monitoring and enforcement being in the hands of Pay.UK.[92] While the PSR's June 2023 Policy Statement acknowledges criticism of the role to be assumed by the operator of the payment system, which was strongly expressed by the

[86] PSR June 2023 Policy Statement (n 6) [3.11] stating: 'We expect the CRM Code requirements to stay in place until the new reimbursement requirement comes into force'.

[87] PSR June 2023 Policy Statement (n 6) [3.10].

[88] PSR June 2023 Policy Statement (n 6) 6.

[89] PSR June 2023 Policy Statement (n 6) [5.32].

[90] PSR Consultation Paper (n 1) [4.31]–[4.32], drawing attention, inter alia, to the FCA's general 'high level' guidance on gross negligence and the risk of a 'tick-box' approach to this test.

[91] PSR June 2023 Policy Statement (n 6) 30.

[92] PSR June 2023 Policy Statement (n 6) ch 8 states that the PSR will continue to work with Pay.UK to develop Pay.UK's role, and that the PSR will publish a review of the new reimbursement requirement within two years, covering Pay.UK and industry's 'implementation' and 'governance', but it does not provide further detail.

House of Commons Treasury Committee,[93] the PSR maintains the view that Pay.UK 'is the appropriate body, in the long term, to make, maintain, refine, monitor and enforce compliance with comprehensive scheme rules that address fraud risk in the system'.[94] Pay.UK's role of monitoring and refining compliance with the new scheme is certainly a vital one. Once the scheme is implemented, the outcomes will need careful, contextual monitoring and review, not least to evaluate whether any evidence of moral hazard emerges.[95] Further, this scheme is designed not only to reimburse customers in certain circumstances, but also to incentivize payment service providers to tackle fraud more aggressively (for example, the default 50–50 sharing of reimbursement costs is designed to incentivize receiving banks to do more to tackle fraudulent payments)[96] and these outcomes will also need careful review. While Pay.UK would be far from the first private sector-led entity to be placed at the heart of a mandatory regulatory scheme for the financial markets,[97] further transparency around these critical post-implementation aspects of the scheme, and in particular around the PSR's supervisory role as regards Pay.UK's expanded responsibilities, is certainly needed pre-implementation.

The debate about Pay.UK's role in relation to this mandatory scheme ultimately relates back to the FMSA's focus on FPS. As discussed above, the FSMA expressly defines a 'qualifying case' of APP fraud for this purpose as one executed over FPS, and requires the PSR, which oversees some, but not all, of the payment infrastructure in the UK, to act accordingly. While the CoP service is a 'payments agnostic overlay service'[98] and the PSRegs for unauthorized transfers are also broadly drafted to cover payments made across different infrastructures, it is a defining feature of the new PSR reimbursement scheme that it applies to one payment infrastructure only. The significant implications of this design are considered in the following section.

3. Coverage

The roll-out of the PSR's new scheme will mean the customers of many more payment service providers are covered by a reimbursement regime for APP frauds than at present. At the same time, however, the scheme entrenches the problem of a piecemeal regulatory response to the risk of APP fraud. More specifically, the coverage of the new PSR scheme is limited in three important ways:

- **By customer**: the PSR scheme only covers consumers (meaning individuals acting other than for the purposes of trade, business or a profession), micro-enterprises, and smaller charities; some small and medium-sized businesses and also larger enterprises, including larger charities, will therefore fall outside the scheme.[99]

[93] The House of Commons Treasury Committee observed in its February 2023 report that Pay.UK is an 'industry body' taking the form of a company limited by guarantee, not a regulator, and that its 42 guarantors include banks, building societies, and other types of payment services providers, therefore finding that Pay.UK has 'inherent conflicts of interest' in terms of administering the reimbursement scheme. House of Commons Treasury Committee (n 47) [16], [23].

[94] PSR June 2023 Policy Statement (n 6) [1.11].

[95] The PSR June 2023 Policy Statement reports that the risk of moral hazard was raised by industry during consultation but that no 'quantitative evidence' was provided to back up these 'assertions'. The PSR points to the gross negligence standard and claim excess as appropriate means to encourage customers to proceed with caution when making payments. PSR June 2023 Policy Statement (n 6) 33.

[96] These new default loss-sharing rules are designed to impose a much higher proportion of losses on receiving banks, ie those holding the accounts used by fraudsters, than at present and thereby create 'adequate incentives to detect frauds and prevent fraud losses'. PSR Consultation Paper (n 1) [5.7] and ch 5 generally.

[97] Another example is the G20-led mandatory clearing requirement, implemented in legislation worldwide the aftermath of the global financial crisis, which requires certain parties to clear derivatives in scope using private entities, central counterparties, with the resulting public-private dynamic discussed in-depth in David Murphy, *Derivatives Regulation: Rules and Reasoning from Lehman to COVID* (OUP 2022).

[98] Pay.UK, 'Confirmation of Payee, FAQs', under the heading 'What payment types are covered by Confirmation of Payee?' <https://www.wearepay.uk/what-we-do/overlay-services/confirmation-of-payee/faqs/>.

[99] A micro-enterprise is defined in the PSR scheme as an enterprise that employs fewer than 10 people and whose annual turnover and/or annual balance sheet total is under 2 million euros; charities are only covered if they have an annual income

- **By payment system**: the PSR scheme will cover payments executed over FPS only, not those made over other infrastructure such as CHAPS, or internal transfers. All three (FPS, CHAPS, and internal transfers) are expressly covered by the CRM Code.[100] Neither the Code nor the PSR scheme covers payments by cash, cheque, direct debit or credit, or credit/debit/prepaid cards.
- **By payment type**: FPS operates between UK bank accounts for sterling denominated transfers only.[101] Payments to an overseas account, and/or denominated in other currencies apart from sterling are therefore not covered by the scheme.

Before going further, it is relevant to note that the PSR consistently refers to its scheme as providing 'minimum standards'.[102] Payment service providers may, of course, act voluntarily to address APP fraud involving the different payment scenarios noted above, while powerful clients outside the scheme may be able to protect themselves through negotiated terms. Furthermore, it is important to note that the loss allocation provisions which are the focus of this article form part of wider, ongoing efforts by regulators to encourage banks and customers to prevent frauds in the first place, for example through intelligence sharing between payment services providers.[103] Nonetheless, discrepancies around payment systems and types created by the specific regulatory scheme implemented under the FSMA remain a significant problem, not only for ordinary individuals out of scope, but also for payment services providers navigating rules on a system-by-system basis.

As explained above, the vast majority of APP fraud currently involves FPS payments, however, there are significant levels of APP fraud cases by value and volume that will fall outside the boundaries of the new scheme. For example, data for the first half of 2022 show that international payments, not covered by any current or proposed reimbursement scheme, were the second largest type of APP fraud by value (£12.9 million);[104] meanwhile, BACS, the 'direct debit' and 'direct credit' payment system, saw the fastest growing number of APP frauds as between the second half of 2021 and the first half of 2022, up 24 per cent by value and 32 per cent in terms of the number of cases. Furthermore, CHAPS, which is not covered by the new scheme, is the UK payment system used for high-value retail and wholesale transactions, settling 0.5 per cent of UK total payments by volume but 92 per cent of total sterling payments by value, turning over the annual UK GDP every six working days.[105] Reflecting the high value of transfers using CHAPS, it represents a relatively small, but significant, subset of APP frauds, at 0.2 per cent by number but four per cent by value. It is therefore clear that there are serious losses suffered to APP fraud involving transfers other than those executed on FPS.

The PSR has already acknowledged the need to level-up protections across different systems,[106] but its own capacity to do so is limited in several respects. First, the PSR only has regulatory powers over UK payment systems, and these powers do not extend to cross-border payments.[107] In terms of UK payment systems, the PSR owns and operates the payment system

of less that £1 million. PSR June 2023 Policy Statement (n 6) Glossary. Business can of course fall victim to APP fraud: see, eg, *Tidal Energy Ltd v Bank of Scotland plc* [2014] EWCA Civ 1107, which involved a corporate victim using CHAPS.

100 CRM Code DS1(2)(a).

101 Pay.UK, 'Faster Payments Service Principles: A Guide for Prospective FPS Participants' (Version 7.4, 7 March 2022) 15.

102 PSR June 2023 Policy Statement (n 6) 35; [7.5]; [7.10]; 61.

103 See, eg, PSR information about the 'wider set of changes' it is implementing, in addition to the FPS scheme, at PSR's APP scams webpage, at <https://psr.org.uk/our-work/app-scams/>.

104 These and other figures for value and number of APP fraud by payment system in this paragraph are from UK Finance 2022 Update (n 3) 35.

105 Bank of England, 'What is CHAPS?' <https://www.bankofengland.co.uk/payment-and-settlement/chaps>.

106 PSR June 2023 Policy Statement (n 6) [2.15].

107 The regulatory powers of the PSR as regards different types of payments are helpfully explained in PSR, 'Authorised push payment (APP) scams: Call for views' (CP21/3) (February 2021) [2.8].

BACS, and it reports that it will consider the risks in relation to APP fraud involving this system,[108] but it is not well-placed to act as regards other payment systems. It is not the regulator of CHAPS, for example, which is operated by the Bank of England, and it has no regulatory oversight of internal bank transfers. The Bank of England falls outside the FSMA, though the PSR June 2023 Policy Statement confirms that the PSR is working on a reimbursement model for CHAPS along with the Bank of England, which it states 'is committed to achieving comparable outcomes'.[109] The Bank of England has also confirmed that it is committed to introducing a scheme for consumer transactions using CHAPS that is 'comparable' to that under discussion for FPS.[110] This commitment is to be welcomed, and suggests that there may be scope for further loss allocation schemes for APP fraud to be introduced even without new legislation to this effect. However, this system-by-system approach risks piecemeal measures. There should, at least, be a single point of oversight to promote co-ordination and transparency, for example around standards of customer care, timeframes, processes, and dispute resolution. As discussed above, the PSR has a limited remit, suggesting that this oversight should be provided by a regulator able to take a more systemic view, ideally supported in this work by more extensive and comprehensive legislation than is currently provided in the FSMA (as discussed above, the FSMA currently only provides for the FPS scheme, and does so by requiring the PSR to act). In the absence of a single body with regulatory oversight of the position applicable to a broader range of payment scenarios, there is the risk that piecemeal arrangements emerge in response to APP fraud. Such arrangements, in turn, might be unduly complex for payment services providers, potentially detracting from initiatives to tackle fraud, and opaque and difficult for customers to navigate.

There are three further factors which support a more co-ordinated approach to the development of loss allocation schemes for APP fraud. First, without robust overall co-ordination, victims may find themselves in starkly different positions as regards reimbursement by their bank because of factors which, from their perspective, appear arbitrary or opaque, for example, a fraudster's instruction to someone in the process of purchasing a house to use CHAPS or to send money abroad.[111] Secondly, as has been established earlier in this article, fraudsters engaging in APP scams are highly adaptive, both in terms of exploiting new technology and instructing victims to bypass checks in the payment journey. Consequently, if mandatory reimbursement schemes do incentivize banks to introduce improved anti-fraud measures for payments in scope, it may simply encourage scammers to conduct APP fraud using less protected payment systems where such schemes are not in place.

Thirdly, without proper, centralized co-ordination, a system-by-system approach to designing and implementing reimbursement schemes for APP fraud may lead to increasingly fragmented rules over time, because the payments sector has enormous potential for innovative change, new entrants, and more diverse methods of payment. As Booysen has put it, in a different context, 'Payment systems are matters of national interest, and payment architecture influences economic success. It is accordingly vital for jurisdictions to continuously position themselves for the benefit of their economy and inhabitants.'[112] However, payments regulators risk chasing their own tail as they seek to support innovation and promote competition in the sector,

[108] PSR June 2023 Policy Statement (n 6) [2.22].

[109] PSR June 2023 Policy Statement (n 6) [1.4] and [2.20].

[110] Letter from Dave Ramsden, Deputy Governor, Markets and Banking, The Bank of England to Harriett Baldwin MP, Chair of the Treasury Sub-Committee on Financial Services Regulation (8 June 2023) <https://committees.parliament.uk/publications/40547/documents/197730/default/>.

[111] As in *Philipp v Barclays Bank UK plc* [2023] UKSC 25, considered in section V.

[112] Sandra Booysen, 'Cheques: to be or not to be?' (2018) Journal of Business Law 283, 298. See also the introduction of promotion of competition into UK regulators' operational objectives discussed in n 20.

while also trying to address the implications for the victims of APP fraud in a system-by-system fashion. Therefore, the current debate needs to consider loss allocation across both incumbent *and* emerging payment systems. Finally, a more centrally co-ordinated approach to loss allocation for APP fraud should also factor in the role of private law and, specifically, the relationship between gaps in regulatory schemes and the availability of private law remedies. As such, the very limited capacity of English private law to fill regulatory gaps in this context is explored in section V.

V. PRIVATE LAW CONTEXT

In some cases, victims of APP fraud use private law to claim against the banks involved in their transfer.[113] These cases highlight how private law has the potential to serve as a 'backstop' for regulatory schemes in this area, as it has in others,[114] meaning that the effectiveness of the regulatory response to APP fraud needs to be evaluated in this wider context. However, as this section of this article shows, the capacity of English private law to serve as a backstop for APP reimbursement schemes is now extremely limited, with the scope of the so-called 'Quincecare' duty of care having been definitively addressed by the Supreme Court in 2023.

1. Quincecare

The 1988 first instance decision in *Barclays v Quincecare* has been pivotal in recent APP fraud litigation, even though it did not itself involve this type of fraud. In this case, the company provided a mandate to its bank, which required the bank to comply with orders that were signed by two executive directors of the company or the chairman alone. On the chairman's instructions, the company's bank paid out £340,000 of a loan which had been made to the company, which was then misapplied by the chairman. In response to the bank's claim for repayment of the loan, the company counterclaimed that the bank was in breach of a duty of inquiry that arose where a customer's instruction should have raised questions in the mind of a reasonable banker.[115]

The starting point for Steyn J's analysis in *Quincecare* was that, when a bank receives a customer's instructions to transfer money from their account, the bank should be 'entitled to treat a customer's mandate at its face value save in extreme cases',[116] such as obvious dishonesty. In these respects, the decision is uncontroversial; the difficulties with the decision emerge as Steyn J proceeded to consider what 'lesser state of knowledge on the part of the bank will oblige the bank to make inquiries as to the legitimacy of the order'.[117] This part of the judgment did not merely qualify the bank's core duty to execute customer's instructions by expanding on what doing so with 'reasonable skill and care' means in this context, but it is framed by reference to a *new* duty upon banks, thereby setting up the potential for a conflict.

The decision proceeds by setting out what it describes as a 'sensible compromise' in cases alleging the misappropriation of a company's money by a director or officer, namely that:

> . . . a banker must refrain from executing an order if and for as long as the banker is 'put on inquiry' in the sense that he has reasonable grounds (although not necessarily proof) for

[113] Reflecting victims' reality as well as the assumption in the regulatory debates, this discussion proceeds on the basis that recovery from the fraudsters themselves is not feasible.

[114] For other examples, see Jo Braithwaite, *The Financial Courts: Adjudicating Disputes in Derivatives Markets* (CUP 2021) ch 4, on the relationship between regulatory schemes of redress and private law duties in mis-selling cases involving complex financial products.

[115] *Barclays Bank plc v Quincecare Ltd* [1992] 4 All ER 363, 374.

[116] *Lipkin Gorman (a firm) v Karpnale Ltd and another* [1992] 4 All ER 331, 349f (Alliot J), cited in *Barclays Bank plc v Quincecare Ltd* [1992] 4 All ER 363, 375.

[117] *Barclays Bank plc v Quincecare Ltd* [1992] 4 All ER 363, 376.

> believing that the order is an attempt to misappropriate the funds of the company . . . And the external standard of the likely perception of an ordinary prudent banker is the governing one.[118]

This has subsequently become known as the 'Quincecare duty', but, as later cases have shown, framing the bank's obligations during the payment process in terms of these competing duties sets up a conflict and detracts from a bank's strict duty to follow authorized instructions. Indeed, as this 'new' duty has come to be widely applied, *Quincecare* has received renewed critical scrutiny. In particular, Professor Watts has powerfully criticized the decision and later authorities where it has been applied, on the basis that that 'Banks are not agents vested with discretionary authority',[119] and arguing that *Quincecare* wrongly applied a negligence rather than dishonesty standard, thereby undermining a bank's strict duty to follow the instructions of mandataries.[120]

2. Application of *Quincecare*

Though *Quincecare* made little impact for several decades, it eventually came to be featured in a line of landmark corporate fraud cases, some of which sought to extend its scope in significant ways.[121] The common denominator in these cases was that each involved allegations of fraudulent instructions provided by an agent of the account-holder; none involved duly authorized instructions from an individual account-holder to their bank. However, in a jump which was, potentially, of systemic importance for the banking sector, an individual victim of APP fraud recently based a claim against her own bank upon an extended version of the 'Quincecare duty'.

The underlying facts in *Philipp v Barclays* are not only extremely unfortunate for the fraud victim, but also show how arbitrary features of a fraud can affect the types of redress potentially available. In this case, the victim and her husband had been tricked into believing that they were co-operating with the UK financial authorities. Ultimately, Mrs Philipp transferred £700,000 to fraudsters, which was the bulk of the couple's life savings. The case fell outside the CRM Code because the Code was introduced more than a year after these payments were made, and, even if it had been in place at the time, the case would not have been covered, because the sums were transferred to an overseas account.[122] The central claim brought against the victims' bank was therefore framed in private law, asserting that the bank was in breach of its 'Quincecare duty' owed to Mrs Philipp, ie, that the bank should be liable for carrying out the client's instructions when, it was alleged, the bank had reasonable grounds for believing she was being defrauded.[123]

While, at first instance, the court awarded the bank summary judgment,[124] the Court of Appeal agreed with Mrs Philipp that her bank owed both a duty to execute her orders promptly, and a duty 'in tension' with the first, based upon *Quincecare*.[125] The Court of Appeal found

[118] *Barclays Bank plc v Quincecare Ltd* [1992] 4 All ER 363, 376.

[119] Peter Watts, 'The Quincecare duty: Misconceived and misdelivered' (2020) 5 Journal of Business Law 403, 416.

[120] Watts (n 119), discussing (inter alia) *Westpac Banking Corp v MAP & Associates Ltd* [2011] 3 NZLR 751, [2011] NZSC 89. This New Zealand case analysed by Watts includes the warning of introducing 'inconvenience and uncertainty' into the bank–customer relationship, thereby undermining 'security of contract in this field'. *Westpac v MAP* [2011] NZSC 89 [11].

[121] Including: *Singularis Holdings Ltd v Daiwa Capital Markets Europe Ltd* [2019] UKSC 50; *JP SPC 4 and another v Royal Bank of Scotland International Ltd* [2022] UKPC 18; *JP Morgan Chase Bank NA v Nigeria* [2019] EWCA Civ 1641.

[122] *Philipp v Barclays Bank UK plc* [2021] EWHC 10 (Comm) [8].

[123] A 'fallback' claim was also made, based on the bank's alleged failure to take adequate steps to recover the sums transferred once alerted to the fraud; the Supreme Court did not consider this argument in-depth because the appeal was from a decision on summary judgment but held that this part of the case could not be decided summarily. This aspect of the decision is not considered further here. *Philipp v Barclays Bank UK plc* [2023] UKSC 25 [115]–[120].

[124] *Philipp v Barclays Bank UK plc* [2021] EWHC 10 (Comm), describing extending the Quincecare duty beyond the case of an agent fraudulent providing instructions to the bank as 'unprincipled and impermissible', [184].

[125] *Philipp v Barclays Bank UK plc* [2022] EWCA Civ 318 [27]. The Consumers' Association, Which?, intervened in the appeal to support the application of the Quincecare duty in this context: its intervention and the appeal generally are considered in David McIlroy and Ruhi Sethi-Smith, 'Bankers' liability for Authorised Push Payment fraud: The evolution

that the underlying reasoning in the authorities was 'quite simple', and designed to 'protect the customer',[126] regardless of whether the instructions came direct from the customer or from their agent. The Court of Appeal's decision may have been regarded as a 'landmark decision' for consumers and companies alike,[127] but it was also quickly criticized in the scholarly literature, on the basis that the clash created with the bank's strict duty to meet a customer's instructions was both mistaken and unworkable.[128]

Indicating the issue's system-wide importance, an appeal was heard by Supreme Court which, in July 2023, unanimously found for the bank. The Supreme Court held that the extended application of the 'Quincecare duty' underpinning the Court of Appeal's decision was 'inconsistent with the first principles of banking law', a central feature of which is the strict duty to execute a customer's authorized instructions.[129] In a decisive judgment, tracing these principles back through the authorities and identifying flawed reasoning in *Quincecare* itself, the Court confirmed that the 'Quincecare duty' is better characterized not as a separate duty but rather as 'simply an application of the general duty of care owed by a bank to interpret, ascertain and act in accordance with its customer's instructions', which only applies where a bank is 'put on inquiry' that instructions from an agent, or someone acting on the customer's behalf, may not be authorized by the customer.[130] In this scenario, a bank is required to take further steps to check that it is following proper instructions;[131] but, by contrast, the Court was unequivocal that that 'these principles have no application to a situation where, as in the present case, the customer is the victim of APP fraud' because here, 'the validity of the instruction is not in doubt'.[132]

The Supreme Court's decision in *Philipp* therefore hinged on the distinction between internal fraud, where, expressly based on principles of agency law, the Court held that the Quincecare duty may apply,[133] and APP fraud, where it was held to have no place. This narrowing of the Quincecare duty, accompanied by the observation that the allocation of losses flowing from APP fraud 'is a question of social policy for regulators, government and ultimately for Parliament to consider'[134] has had a mixed reception. In some quarters, the decision has been welcomed precisely because of its narrow focus on the legal principles, being described as a 'welcome clarification bringing long-awaited steps towards legal certainty', after earlier cases had veered

of the Quincecare duty' (2022) 37(5) Journal of International Banking and Financial Law 304. Note that one of the authors of the JIBFL article referenced here was instructed by Which? in this appeal.

126 *Philipp v Barclays Bank UK plc* [2022] EWCA Civ 318 [28] and [29].

127 McIlroy and Sethi-Smith (n 125) 306.

128 See, eg, Rui Yuan Chua, 'The Quincecare duty: an unnecessary gloss?' (2023) 3 Journal of Business Law 161; and Peter Watts, 'Playing the Quincecare card' (2022) 138 LQR 530.

129 *Philipp v Barclays Bank UK plc* [2023] UKSC 25 [3].

130 *Philipp v Barclays Bank UK plc* [2023] UKSC 25 [97]. This will ultimately depend on the facts of the case, but some examples are provided in Jonathan Davies-Jones KC and Alexia Knight, 'When is a bank put on notice of an agent's fraud?' (2023) 38(10) Journal of International Banking and Financial Law 664, 666.

131 *Philipp v Barclays Bank UK plc* [2023] UKSC 25 [97]. Though it falls outside the scope of this article, there is much to consider in terms of how *Philipp* may affect the operational processes banks should follow when dealing with mandataries. For practitioner consideration of the 'key practical takeaways' from the decision, see Clifford Chance, 'Philipp v Barclays—UK Supreme Court overrules Court of Appeal on Quincecare in Landmark Return to Basics of Banking and Agency Law' (July 2023) <https://www.cliffordchance.com/briefings/2023/07/philipp-v-barclays-uk-supreme-court-overrules-court-of-appeal.html>. See also Piers Reynolds and Laura Feldman, 'Steps towards legal certainty' (2024) 140 LQR 176, 181 on issues requiring clarification post-*Philipp*.

132 *Philipp v Barclays Bank UK plc* [2023] UKSC 25 [100].

133 It has been pointed out that one consequence of this aspect of *Philipp* is the increased significance of the governing law of the agency relationship, discussed in the context of corporate customers in Matthew McGhee, 'Quincecare, agency and conflict of laws: what law do we look to?' (2024) 3 Journal of International Banking and Financial Law 166; while the underlying differences between several common law jurisdictions in this area are explored (with reference to the Court of Appeal's subsequently reversed decision in *Philipp*) in Matthew McGhee, 'Different jurisdictions' approaches to Quincecare: England and Wales lead the expansive approach' (2022) 37 Journal of International Banking and Financial Law 674.

134 *Philipp v Barclays Bank UK plc* [2023] UKSC 25 [6].

too far into the area of policy.[135] However, the decision has also been criticized for incorrectly framing the question about the scope of the Quincecare duty as 'a choice between principle and policy', rather than engaging with the 'extent and degree' of implied qualifications to the bank's duty to fulfil payment instructions.[136]

That the Supreme Court in *Philipp* emphasized its distance from 'social policy' questions around the reimbursement of victims of APP fraud, which, as we have seen, are of system-wide relevance and, as the judgment itself noted, were concurrently being considered by legislators and the PSR, is perhaps not surprising.[137] Nonetheless, *Philipp* did have significant implications for the regime of loss allocation for APP fraud, because the decision left individuals outside the PSR scheme unable to base an alternative claim against their banks on the Quincecare duty[138] and therefore, in the words of one review of the case, 'high and dry'.[139] In this context, the relationship between the court and legislators is more interconnected and more dynamic than the decision in *Philipp* suggests. Given that several other private law routes had already proved unsuccessful for victims of push frauds,[140] *Philipp*'s removal of this private law backstop for individual victims of APP fraud has, at a time when this kind of bank fraud is proliferating, increased the urgency of legislators developing a more centrally co-ordinated regulatory response to APP fraud than has emerged to date. Whether a loss allocation regime applies to a particular payment should not turn on factors which may well be arbitrary for victims and/or deliberately chosen by fraudsters.

VI. CONCLUSION

The background to this article is a relentless surge of APP fraud, catalysed by radical changes underway in the banking and payments sector. As this article has shown, this is a type of fraud where all may be vulnerable, where fraudsters are exploitative and adaptive, and where the default position facing victims is a legal and regulatory lacuna. Accordingly, it is right that APP fraud has received considerable attention from consumer groups, industry associations, and regulators since 2016, but also that the mix of regulatory schemes now being implemented receives proper scrutiny. Moreover, given the UK regulator's recent observation that 'other jurisdictions are watching [the UK] closely in considering their own approaches', evaluating the UK's new statutory response to APP fraud has even wider relevance.

By shedding light on the default legal position governing different types of bank fraud, the patchwork of goodwill payments to victims and limited scope of voluntary reimbursement schemes, this article has drawn attention to the importance of improving certainty and consistency for parties affected by APP fraud. To the extent that the UK's new mandatory reimbursement scheme will indeed bring in a clearer, more detailed and consistent framework, with

[135] Reynolds and Feldman (n 131) 180. On the same lines, see Mark Hsiao, 'Bank's Quincecare duty and banks' duty to execute order: a welcome clarification' (2024) 39 Journal of International Banking Law and Regulation 199, welcoming the 'strict clarification' in the decision.

[136] John Yap and Joseph Khaw, 'Philipp v Barclays Bank UK Plc in the UK Supreme Court: The Quincecare duty as a "special or idiosyncratic" term implied in law' (2023) 38 Journal of International Banking Law and Regulation 460, 466.

[137] *Philipp v Barclays Bank UK plc* [2023] UKSC 25 [21], referencing the proposed reimbursement scheme under the Financial Services and Markets Act 2023.

[138] As reflected in some newspaper reporting of the decision. See, eg, Noah Eastwood, 'Banks off the hook over payment fraud after Supreme Court case' *The Daily Telegraph* (13 July 2023).

[139] David McIlroy and Ruhi Sethi-Smith, 'No point preventing fraud? *Philipp v Barclays Bank*' (2023) 38 Journal of International Banking and Financial Law 513, 513; the article goes on (at 516) to describe the Supreme Court's decision as 'disappointing for consumers' and a 'cause for concern' given that banks were not compelled 'to take reasonable steps to prevent APP fraud'.

[140] See, eg, *Jeremy D Stone Consultants Ltd and Jeremy Stone v National Westminster Bank plc and Paul Aplin* [2013] EWHC 208 (Ch) and more recently, a case brought by a company operating in Saudi Arabia that was the victim of APP fraud, with sums paid to the UK account held by the fraudster with the defendant bank: this claim was brought on the basis of knowing receipt and unjust enrichment of the bank, and was unsuccessful on each basis: *Tecnimont Arabia Ltd v National Westminster Bank plc* [2022] EWHC 1172 (Comm).

some features in line with that for unauthorized payments, its provisions will be of considerable value for victims in scope. While the new scheme covers the payment system used for the vast majority of APP fraud at present, this article has also found that, without overall co-ordination, a 'system-by-system' approach to rolling out a regulatory response to APP fraud raises significant problems. As we have seen, gaps in regulatory coverage create complexity for all stakeholders, while perpetuating inconsistencies. From a fraud victim's perspective, potential routes to redress should not turn on factors such as the type of payment infrastructure used to defraud them; neither is it efficient for payment service providers engaged in billions of transactions to administer many diverse reimbursement procedures, defences, and definitions. Moreover, incentives to roll-out better anti-fraud measures should apply consistently or risk opening new opportunities for fraudsters.

This article has also shown that a centrally co-ordinated regulatory response to APP fraud would be better placed to manage the fact that the payments sector is evolving rapidly. Diversification, innovation, and greater competition in the sector are already opening up new and valuable possibilities for consumers and businesses alike, but they also risk the current 'system by system' approach to this type of fraud fragmenting further.

Finally, this article has demonstrated that the effectiveness of regulatory schemes of redress for bank fraud must be evaluated in their wider legal context, specifically, by taking proper account of the capacity of private law to provide meaningful routes to redress. Where private law offers those falling out of scope of regulatory protections a reasonable and realistic means of redress, it may potentially serve as a 'backstop'. However, as discussed above, under English private law at least, there is now no backstop based upon a 'Quincecare' duty of care for individuals providing payment instructions to their bank on their own behalf. Taking account of the wider legal context therefore adds a further, important reason to work towards more joined-up regulatory coverage for this kind of bank fraud. For other jurisdictions engaged in similar debates as in the UK, evaluating the wider legal context should also be factored into the process of designing an effective and co-ordinated regulatory response to the evolving threat of APP fraud.