# PSR Consultation CP23/4:

## A new reimbursement requirement

## Faster Payments APP scam reimbursement rules and operator monitoring

## Legal Structure

**Ordo response**

Submission to: appscams@psr.org.uk by 5pm 25 August 2023

**PUBLIC**

# Introduction

## What does Ordo do?

Ordo's fully hosted and customisable open banking-enabled payments managed services provide businesses – large and small – with low cost, highly secure, real-time and easy to use Request to Pay, e-commerce, Point of Sale/QR Code, invoice and contact centre payments direct from their customer's ASPSP accounts into their own ASPSP accounts for both single and recurring payments.

Businesses can access the Ordo managed service in a number of ways: though an Ordo Merchant Acquirer/PSP payments partner, such as Pay360 or Contis, directly via Ordo's business level APIs, and for smaller businesses, through our integrations with QuickBooks, Sage, and Xero accounting software or via Ordo's web/app interfaces.

Ordo also uses open banking to enable refunds and secure customer pay outs as well as account validation services and has fully managed VRP enabled services, initially for sweeping, allowing businesses to take advantage of the latest open banking technology with minimal development and integration effort.

Ordo's cloud hosted managed service is fully white labelled allowing business's own brand and look & feel to be incorporated into all customer interactions, giving a consistent customer experience but without the overhead of developing and keeping up to date their own open banking customer journey.

## *Who are Ordo?*

Ordo was founded by the former management team of the UK's Faster Payment Scheme in 2018 to use Open Banking payments to provide businesses with a much-needed alternative to slow, high-cost card payments and insecure direct ASPSP payments. Ordo is authorised by the Financial Conduct Authority as an Authorised Payments Institution to carry out Account Information Services and Payment Initiation Services (FRN 836070). Ordo is backed by private investors, Nationwide Building Society Ventures and CGI, the global IT services business.

*Consultation response*

We are pleased to see the PSR consulting on the structure for the compulsory reimbursement of APP scam victims.

APP scams are a growing concern and, along with anti-fraud measures we have built into our service, we want the ecosystem to evolve holistically to prevent and stop this fraud, which can have a lasting negative impact on victims both financially and otherwise.

We look forward to evolution of this regime, to a structure which firstly, places the greatest liability on the party most at fault and with the richest most accurate view of customer activity to determine uncharacteristic, unlawful and/or inappropriate behaviour (the receiving bank operating bank account services for fraudsters), and secondly, enabling signalling to consumers to adopt more secure methods of payment, like Open Banking, rather than traditional less technologically advanced methods.

**Question 1:** Does our proposed package of the three legal instruments outlined above (and published in the annexes to this document) give full effect to the policy set out in our policy statement PS23/3? If not, why, and what changes are necessary in order for it to do so?

We do not agree the three legal instruments will achieve the policy intent as set out in policy statement PS23/3 and successfully combat APP fraud in the UK.

**De-risking**

We believe the 50/50 sending and receiving bank liability model will cause *all* banks to query *all* payments irrespective of their risk whereby *hindering payments*, and threatening the Open Banking market, *rather than stopping fraud*.

FinTechs providing innovative services to business and consumers in the Open Banking market already face banks limiting, adding friction and blocking legitimate Open Banking payments. Imposing equal liability on both sides of the transaction will only increase the rate of blocking from double the number of banks (now on both sides of every transaction), making it hard for Open Banking to be a reliable service, and making it untenable as a competitor to cards.

As we have previously outlined to the PSR, it is our reasoned view that far more liability (if not 100% liability) should be on the receiving bank, the entity who has KYC-ed a fraudster, which is providing bank account services to a criminal, and is breaching its ongoing AML obligations. In addition, it is the receiving bank that has a richer and more accurate view of what the account should be used for, and the frequency and amounts that are likely to be received into the account, as well as the history of received payments, affording the receiving bank a rich, unique and insightful view of usual and expected bank account activity, or otherwise.

Placing liability on the sending bank incentivises banks to stop payments, not prevent fraud. Placing liability on the receiving bank incentivises banks to conduct proper due diligence of their customer and appropriately monitor received funds, preventing fraud. The rate of false positives that result from sending bank liability will be, and is, huge, and it will not catch what banks deem as acceptable risk – lower value payments, but which are still significant and damaging amounts to lose for victims. Conversely, receiving bank liability, due to the fuller view the receiving bank has, will catch all values of fraud, with false positives having a much lesser impact. Indeed, where a receiving bank is suspicious of an amount received, the receiving bank can ring fence the funds

pending its further investigation; whether found fraudulent or not, the payment has been made; if fraudulent, the criminal rightly never receives the funds and these can be repatriated in full with nearly all harm averted, and where the payment was not fraudulent, funds can be released to the receiving customer at a slight delay.

**User experience**

Where banks do not block Open Banking payments, the current proposals are likely to incentivise banks to introduce additional friction in instant payment journeys (including those initiated by Open Banking), such as more screens, 'pop up' warnings and/or verification steps for consumers when authenticating payments. This is inappropriate for Open Banking payments, as opposed to Faster Payments, as the PISP indelibly populates the Open Banking request for payment, giving the payer the exact account title of the entity asking them to pay, and meaning the payer is not responsible for inputting receiving account data.

**Status of the policy**

Following input from industry on this matter, should it be the case that there is enough doubt as to the effectiveness of this proposal, we would support a full risk assessment of the proposed measures, and alternatives, being conducted by an independent body.

In the event this policy stands for the immediate term, we look forward to it evolving, as has been the stated intent, to be more effective at stopping fraud, not payments, and better reflect the information available and appropriate behaviour of ecosystem participants; this includes the model evolving to rectify the situation proposed which results in a PISP acting as a receiving PSP bearing *all* the liability for the receiving PSP, leaving the PSP with evidenced poor KYC processes and allowing a criminal to collect stolen funds bearing zero liability.

We have no comments on the effectiveness of the legal construct specifically.

**Question 2:** Do you agree with our proposed timeline for implementation and the feasibility of the 'go live' date of 2 April 2024? If not, why and what alternative would you propose?

Given our comments in answer to question 1 above, we would support a full review of the proposals, and alternatives, by an independent body. Should this be progressed, this would impact the proposed implementation timing.

In the absence of review, we agree the proposed timeline for implementation with a 'go live' date of 2 April 2024. This is an important legal apportioning and enforcement of liability which, through its evolution, seeks to make good the financial loss of an innocent victim of crime, and which will positively impact how Faster Payments are viewed and used by consumers. Implementation dates will always be claimed to be impossible by those who are not motivated to make changes for the greater good. Decisions on timeline should be based on what a reasonably efficient entity could manage, balancing risk with the opportunity cost of delaying the continued harm that is being suffered by innocent victims.

As we have previously voiced to the PSR and briefly summarised above in answer to question 1, we do not agree that the 50/50 liability split between sending and receiving bank is most appropriate; indeed Chris Hemsley, at the announcement of this policy at the Kings Cross breakfast event on 7

June 2023 acknowledged, this liability model is probably not right for Open Banking payments, and that this liability framework will evolve. This evolved liability model should reflect the information available to each party involved in making payments and the degree to which they have behaved and acted properly to prevent fraud. Therefore, the sooner this first phase of the APP scam liability model is live, the sooner the model can be considered and honed to be a more fairly apportioned and justified liability.

The parties that are resistant to this policy coming into force on 2 April 2024, should it not be reviewed, will be those that do not have confidence in their KYC processes and ongoing AML compliance. The protection of consumers should not be delayed because financial institutions cannot implement and monitor the proceses they are already required to have in place by the FCA and in accordance with AML legislation.

**Question 3:** Do you have any comments on the frequency of reporting to Pay.UK? Would a different reporting frequency strike a balance between the cost and burden of reporting and sufficient data coverage?

The reporting frequency should ensure data should not be so historic as to be worthless. An outcome of reporting should be to be able to intercept should any trends emerge; the frequency of data should be informed to enable this outcome to be achieved, as well as longer term fraud patterns.

The data listed in paragraphs 4.5 and 4.6 would need to be provided less than monthly. These data sets do not seem to be time critical.

However, sharing details of suspicious/fraudulent activity ***is*** time-critical - otherwise there is a risk of the funds being moved on/converted to crypto or similar. We note that onus is on the sending bank to inform the receiving bank; there should also be a provision for receivers of suspicious transactions to notify senders of their suspicion - this also underpins our argument for receiving bank liability.

What is not clear is whether Pay.UK are acting as a post-box for banks to send into, with Pay.UK being post only and delivering onto the other bank(s) involved. If that is part of Pay.UK's role, then twice a day is not frequent enough, rather, it should be as soon as possible. More information and clarity regarding the practicalities of creating and maintaining a process that will prevent fraud is needed; it may be envisaged that Pay.UK are to provide a messaging tool to facilitate this, but this is not clear.

**Question 4:** Do you have any comments on what data Pay.UK should gather?

The number of APP scams reported by consumers, broken down by sending and receiving PSP, would be useful to determine trends and weak participants, if any.

In addition, the need for further data may come out of the need to accommodate PISPs as described as Model B in Annex 2 of the policy statement, where PISPs act as receiving PSPs.

**Question 5:** Do you have any comments on the approach and principles for Pay.UK monitoring compliance?

Pay.UK, as system operator of the Faster Payments system, is a company guaranteed by its participants. Pay.UK management are likely to have limited power of directing its participants, other than the threat of reverting to the PSR, even once the clearing and settlement layer of the NPA is in place. Pay.UK's limited possible courses of action for enforcing non-compliance with regulatory directions are either reputational (PSPs having to report to various committees) which, whilst undesirable, is not a huge deterrent, or prohibiting a participant from continuing to use the system, which is too effectual and damaging to consumers to likely ever to be used; the only other option is to inform the regulator. Directions on participants directly are the regulatory force; the regulatory compliance activity and oversight should be via a direct relationship and not diluted and interpreted.

If the PSR persists with indirect monitoring and compliance, even post NPA, the PSR will need close oversight of APP scam enforcement and the pro-active prevention of fraud which is the desired behaviour from PSPs.

In addition, Pay.UK has no jurisdiction over, and no communication channel with, PISPs, and nor do PISPs have any standing to input into Pay.UK. The Open Finance Association is working to establish a regular dialogue with Pay.UK. Any consultation and establishment of reporting and reimbursement process(es) needs to be wider than only their direct and even indirect participants. Any process put in place to rightly reimburse consumers for APP scams that involve (rightly) PISPs (although the PSP ultimately opening and operating bank account services for a fraudster avoiding liability entirely remains unacceptable and at odds with the PSR's desire to incentivise all parties in the payment chain to combat fraud) must involve PISPs in reporting and communication. Pay.UK and resulting processes must also reflect that PISPs are often smaller with fewer resources than ASPSPs; whilst this means PISPs will often be more responsive and agile, the lesser resource, and different risk appetites, customer care and communications approaches between ASPSPs and PISPs must be considered and accommodated. It would be unacceptable for Pay.UK to manage this responsibility solely through its Rules and Governance committee, or similar, for example. Consequently, a PSR direction must be placed on Pay.UK to involve, consult, consider and accommodate PISPs.

**Question 6:** Do you have any other comments on the section 55 specific requirement on Pay.UK?

Faster Payments rule change requirement, s55 specific requirement - Category 2 changes should still require PSR consent before changing. Comments on principles (Q5) to be considered.

**Question 7:** Do you have any other comments on the section 54 specific direction on Pay.UK?

Compliance monitoring/data collection, s54 specific requirement – Comments on principles (Q5) to be considered.

**Question 8:** Do you have any other comments on the section 54 general direction on PSPs?

There is a need for greater clarity around the scope and obligations for non-bank PSP arrangements, with each business type to be included within the definitions section of the direction, including EMIs and PISPs.

The availability of one, centrally coordinated secure mechanism, used by all in scope firms, to enable the exchange of claim data, to allocate reimbursement and to facilitate large scale

reconciliation of accounts will be essential to the success of the reimbursement model. We suggest the PSR include an obligation on firms to participate in one regulator approved industry data sharing mechanism. Without a direct obligation to participate, the timeline for on-boarding all in scope firms may be protracted.

**Question 9:** Do you agree that it is right to follow a similar approach to imposing a reimbursement requirement within the CHAPS payment system?

Yes.

**Question 10:** Do you have any comments on the most effective way to do this?

No comment.

**Question 11:** Do you have any other comments on this consultation?

No comment.

Should you wish to discuss this matter, please do not hesitate to contact Ordo.