PSR Consultation CP23/7:

Authorised push payment scams

The consumer standard of caution

Ordo response

Submission to: **appscams@psr.org.uk** by 5pm 12 September 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 consumer standard of caution 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.

General response

There has not been enough time given to be able to consider the PSR's specific questions.

Generally, it is crucial that warning messages are tailored and specific. Our experience to date is that in many cases the warnings made by banks are applied too frequently and generically eg some banks even ask the same questions when paying a whitelisted payee, and regardless of amount.

However, apart from where there is a known scam in operation, we argue the sending bank is not the party with the best viewpoint to make a judgement about whether a payment is suspicious or not; and it will instead result in sending banks warning and stopping all payments that will potentially cause them larger liability ie higher value payments, as is the case today.

Requiring a sending bank to give bespoke warning which it is not in a good position to see, causing them to stop a payment will increase the false positives from sending banks, because the only indicator they have for fraud, other than in the instance of a known scam, is size of payment. This will impact commerce through Faster Payments as well as Open Banking. *All* payments irrespective of their risk will continue to be stopped, *hindering payments*, and threatening the Open Banking market, but will ineffectively and by chance stop only some fraud.

Conversely, the receiving bank, the entity who has KYC-ed potentially a fraudster, is providing bank account services to a criminal, and is breaching its ongoing AML obligations, has a richer and more accurate view of what the account should be used for through the account opening process, 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. It is this party that is more informed and accurately able to detect potential fraud, and should hold the responsibility for delaying access to the payee to cleared funds and giving warning to the sending banks to clarify and confirm the legitimacy of payment with its paying customer.

Requiring bespoke messaging that the sending bank is not best placed to see incentivises sending banks to stop payments, not prevent fraud, making payments unreliable and creating mistrust, rather than preventing fraud. Instead, requiring the receiving bank to delay access to funds once a payment has been made 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 banks stopping payments 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.

Receiving bank delaying access to cleared funds whilst warnings are passed to the sending bank and payer allows banks to pick up low value, high frequency fraud as well as high value fraud; this is not possible with the sending bank only giving warnings.

Conversely, the receiving bank carrying out investigations means that where a receiving party has confirmed their legitimacy their bank can learn and know not to hold up payments in the future.

Lastly, how is placing responsibility on the sending bank to give bespoke warnings, presumably requiring a sending bank to monitor and question their customers' payment instructions, compatible with the Supreme Court's July 2023 ruling in Phillipp v Barclays regarding the 'Qunicecare' duty where the court said it was not the place of the bank to question its customers' instructions?

Given the above arguments and our previous communication with the PSR, we look forward to the evolution of this policy to create better outcomes for consumers, particularly for Open Banking where payments are more securely and obviously to legitimate payees.

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