PSR Consultation:

APP Scams

Ordo response

Submission to: **appscams@psr.org.uk** by 5pm 25 November 2022

PUBLIC

The following information is the property of The Smart Request Company Ltd, trading as Ordo ("Ordo") and is provided to you in response to the above consultation only.

*The information is only to be used by you in connection with the consideration of your response to authorised push payment fraud, it is not to be used by you for any other purpose. The **REDACTED** version only may be published in response to this consultation, without alteration.*

This is the REDACTED version of our response and MAY be published.

The commission of any unauthorised act in relation to the information may result in civil or criminal actions being taken by Ordo in relation to this matter. Any licences issued by the Copyright Licensing Agency Limited do not extend to this matter. All opinions and forecasts contained herein are the opinions of Ordo and are made in good faith at the time of publishing.

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 APP scam liability and, particularly, altering the liability model from that which exists under the Contingent Reimbursement Model currently. Going hand in hand with the aim of reducing fraud is ensuring any regulatory interventions encourage and incentivise the right behaviour both from ASPSPs, but also enabling signalling to consumers to adopt more secure methods of payment, like Open Banking, that are available to them today.

50/50 liability proposal and consultation process

Putting aside the role of law enforcement, there are only two parties that can potentially help consumers avoid falling victim to APP scams, the banks involved in sending money under the instruction of the victim and the banks receiving money on behalf of the criminal. As consumers have limited scope to reduce their risk of being defrauded, can be devastatingly affected by the financial losses they incur, and as banks have the greatest opportunity to stop fraudulent payments going to criminals, and greater financial scale to absorb losses on behalf of their customers in the short term, it makes sense to introduce a comprehensive bank funded reimbursement model to remove the financial consequences from consumers and incentivise banks to act to stop APP frauds.

Under the contingent reimbursement model, when reimbursement takes place, this is principally funded by the sending bank on the basis that this incentivises the sending bank to educate and support their customer into not making a payment to a criminal. Whilst this helps in less than half the cases and rarely to the full extent, it also encourages banks to effectively blame the victim for falling victim and be financially penalised (likely coupled with significant psychological detriment).

The PSR has taken on board the suggestion that the receiving bank may also have a role to play and has consequently proposed a 50/50 split of reimbursement funding from the sending and receiving bank. At one level this is welcomed, but simply spreading responsibility in this way on the one hand to be 'fair' to all parties, and on the other, to maximise the potential to stop frauds (belt and braces), while superficially attractive, fails to recognise that there are also consumer and business downsides associated with the steps banks could take to minimise APP fraud. As these actions come at a cost to banks and/or their customers, and could have negative unintended consequences, a more nuanced analysis needs to be undertaken before settling on an equal split of liability between the two banks involved.

To select the most appropriate liability split between the sending and receiving bank it is necessary to consider the information available to each party, the actions available to each party, and what actions the allocation of any liability will cause a party to take. It is not clear from the PSR's consultation that this has been done, and that a broad enough range of allocations has been considered, specifically allocating full liability to the receiving bank.

The sending bank's position

The sending bank (victim's bank) only knows the history and payments patterns of its own customer, so while it may spot an APP scam payment as abnormal due to its size compared to normal payments from the customer, it is very likely to identify many false positives. The infrequent nature of high value consumer payments means that distinguishing between scam payments and legitimate payments (like paying for a car, paying for building work, or making an investment) is very hard for the sending bank due to the very limited information it has access to. Given the limited information available to it the only action available to the sending bank is to interrupt all higher value payments to new payees and seek information from the payer to try and detect a scam. Given the nature of the social engineering used to enable scams, and the fact that this process will have been successful if a customer is about to make a payment to a fraudster, the customer information gathering process can be lengthy and time consuming for both the bank and their customer. As long as the sending bank has some liability for reimbursing a scam payment, it will seek to minimise that liability by discouraging its customers from making such payments, whether scam or actually legitimate. This will continue to make account to account payments harder to execute and particularly get in the way of consumers making higher value Open Banking Payments. Sending banks will never be fans of customer or Open Banking initiated Faster Payments as the bank holds a liability it is not in a good position to mitigate, it

would much rather consumers continued to use cards where, not only is it insulated from liability, it earns significant revenue in the form of card issuer fees.

Putting another barrier in the adoption of open banking and other account to account payments reduces the chances of account to account competing with cards. This lack of competition will mean businesses will continue to pay higher costs for payments, costs ultimately borne by their customers. This is not in the public interest.

To summarise. Sending banks bearing liability for APP scam payments to criminals can only reduce their exposure by trying to prevent their customers paying scammers. A significant side-effect of this action will be to interfere with and make much less attractive legitimate higher value payments forcing payments off high efficiency Faster Payments/NPA onto expensive card payments. The limited available information to sending banks makes false-positives very likely.

The receiving bank's position

By contrast, the receiving bank (the criminal's bank) should have good and growing information about the receiving account, how it is being used, and what person or organisation is running the account. The receiving bank can spot in real time that an account has suddenly started receiving large payments that are inconsistent with the KYC'd purpose of the account, and through KYC should know whether the account is a personal or business account, and if business, what type of business. If the receiving account is a personal account, either opened by a criminal, or a mule account recruited by the criminal, then large receipts will be even easier to spot than large outgoings as they are even more unusual for consumers. The receiving bank also potentially has actions it can take that will mitigate scams, without making Faster Payments too hard to use.

Putting aside tipping-off rules (which might need adjustment or clarifying), the receiving bank, having spotted an unusual transaction could ringfence that transaction on receipt. It can then investigate what the account is being used for, protecting the payer's funds without interrupting the transaction flow and as is the case with sending bank false positives. The bank's enquiries will be focussed either on a criminal scammer/mule, or on a legitimate person or organisation that can easily provide an explanation to the bank for the transaction and then gain access to their funds. Banks already have a clear responsibility to know who their customers are, and what they are using their accounts for to stop Money Laundering.

This delayed availability of funds to a suspicious payee doesn't change the Faster Payments model. The payment has still been received irrevocably and the payee can rely on funds being available unless they are shown to be criminals, in which case they have no rights to the funds anyway and they can be costlessly reimbursed to the victim. If the payee is not a criminal, it is guaranteed that they will receive funds, just after a short delay, and therefore they can supply goods or services to their customer without risk prior to investigations being completed. This means that the impact on transaction flows and businesses and their customers of false positives at the receiving bank end is massively lower than false positives from the sending bank.

False positives will also in themselves be much less likely because the receiving bank has so much better information. The vast bulk of legitimate higher value payments are made to business bank accounts. The receiving bank naturally knowing whether the receiving account is personal or business means most higher value payments, which will go to business accounts, won't need to be reviewed. Higher value receipts into personal accounts can then be focussed on to interdict scam payments. While there will be some false positives, these will be very infrequent for consumers (consumers rarely receive higher value payments other than regular and predictable salary payments). Banks can then quickly contact their customer to establish their bona fides, and if still in doubt can consult the sending bank to validate the sender's comfort with making the payment. Over time, just as banks encourage their customers to notify them in advance of foreign or large card spends, consumers can be encouraged to notify their banks of unusually large receipts. These steps may indeed already be theoretically required of banks to meet their AML obligations.

To summarise. Receiving banks bearing liability for APP scam payments to criminals (their account holders) can reduce their exposure by preventing criminals gaining access to funds paid into their, or their mule's bank account by ring-fencing suspicious receipts until the account holder has been validated. There are very limited down-sides

to businesses and their customers from false positives. The good KYC information available to receiving banks makes false-positives very unlikely for the majority of payments.

Considering the situations of the sending and receiving banks in the round, we believe there is a very strong case to allocate liability for scam payments made to criminals wholly to the receiving bank and not share any of this with the sending bank:

- It is very hard to imagine a scam payment situation where the sending bank can identify it as suspicious, but the receiving bank cannot – there is little incremental benefit of both parties trying to spot suspicious payments.
- There are very limited downsides from receiving bank false positives, and very substantial downsides (including strategic undermining of account-to-account payments as competition to cards) from sending bank false positives – there is a substantial cost to the economy of sending banks also trying to spot all suspicious APP scam payments.

Full liability on the receiving bank will incentivise the *change in behaviour* that will stop fraud, not payments.

Our assumption in this proposed receiving bank liability model is that CoP (or functional alternatives such as presenting the payee account name to the payer prior to payment authorisation) is mandated for all banks, and where CoP is not used by a sending bank, this switches the liability model and makes sender bank 100% liable. The reasoning for this being the sender bank has not kept up with the latest widely available technology and adherence to best practice. This will incentivise ASPSPs to implement CoP, a service that does enable sending banks to reduce scam payments and misdirected payments without false positive downsides.

It is not clear from the consultation that the PSR has considered this model where 100% liability sits with the receiving bank. Given that for all scam payments, the receiving bank is operating an account for a criminal or a criminal mule and should be liable for this, this seems strange.

As a minimum, the 100% liability model on the receiving bank with its pros and cons needs to be fully laid out against the current (100% sender) and a 50/50 model if a good decision is to be made.

In our view, for any proposal to be robustly enforced, it must be evident broader thinking was carried out before reaching and consulting on a single proposal, and how such proposal best achieves desired outcomes.

At this stage, we cannot conclude this has been done or that the best model is being proposed.

Mandatory reimbursement

Ordo agrees with the PSR's proposals to mandate reimbursement in all cases but for gross negligence and where the payer is complicit in the fraud. Mandating all fraud (subject to high bar carve outs) supports the argument that this will incentivise *a change* in behaviour, certainly. As far as a change is desired, the PSR's proposal to mandate compensation of all APP scam fraud (carve outs accepted) satisfies that requirement.

Method of implementation and Pay.UK's role

We agree that an appropriate place for implementing an APP scam liability model would be the Faster Payment Scheme rules. Consequently, and in line with the PSR's stated objectives of having a Payment Systems Operator that is motivated to minimise, and enforce prevention of, fraud, that Pay.UK be the body that enforces this framework and it be empowered to do so.

It is imperative that this expansion of Pay.UK's role in this instance, to be empowered to enforce the further prevention of fraud across the payment system that it runs, does not creep into governing, setting standards or frameworks or similar for services that operate extracted from its payment system and instead in the competitive layer of the payments ecosystem, the Open Banking TPP layer. Any governance at this level, regarding services and

TPPs who provide overlay services and do not touch clearing and settlement, must be governed by a wholly independent body, currently OBIE and what this will evolve into as the Future Entity.

PSR additional legislative powers required

We suggest that whilst the PSR is obtaining its legislative powers to have authority to mandate compensation of all victims of APP Scams, it obtains the legislative authority for the following to enable it to function fully and well:

CoP -

We state above that we propose the 100% receiver ASPSP liability model be switched where there is an APP scam from a sending ASPSP that does not operate CoP or a functional alternative*. This will drive more sending ASPSPs to adopt CoP, but it would also be prudent and in the interests of consumers that all levers are used, and the PSR having the power to mandate CoP on all ASPSPs for the good of society is another such lever.

Therefore, all ASPSPs need to support CoP as a sender or receiver of payments, to negate the defect of CoP today where eg First Direct can only perform a CoP check if the receiving ASPSP also supports CoP.

* E.g., If a PISP presents a payer, via open banking, with the account name of the payee, that has been suitably sourced and validated by the PISP, then there is no incremental benefit to adding CoP to the process. Adding CoP in this circumstance simply complicates the customer journey for no good reason.

'On us' payments -

If the argument is accepted that a victim should be (apart from where high threshold exemptions have been exceeded) compensated, then it is illogical for there to be a gap where a payer has inadvertently sent money, in a scam, to an account at an ASPSP in the same banking group, or even the same banking brand!

The victim is unlikely and cannot be expected to know, and cannot be expected to investigate, the receiving account's banking group. If it's decided that it is appropriate for intergroup receiving ASPSPs to compensate victims, there is no difference to the entitlement of a victim sending money intragroup!

We note that the PSR states it expects compensation to victims for APP scams where the transfer has been 'on us' is to be treated the same as for transfers intergroup, but our view is that this is far too weak and leaves APP scam victims vulnerable to larger ASPSP group companies, the PSR needs to require this.

Unintended consequences

A consequence of actions ASPSPs take to limit their exposure to fraud as a result of mandating APP scam victim compensation is that it could cause fraudsters to move to using cheques. If ASPSPs have weaker controls with cheques than electronic payments, fraudsters will exploit those weaknesses. It should be noted that cheques already put liability on the receiving bank to check the name on the cheque matches the account name (as the paying bank can't control where funds are paid into) and therefore our 100% receiver proposal already has precedent. Therefore, any liability model regarding APP scams should also extend to cheques to ensure APP scams are reduced rather than just moved. (The threat does not transpose in the same way to the remaining payment methods: Bacs – consumers cannot make Bacs payments; Cash – cannot be traced; Cards – alternative compensation models).

Other PSR Consultation points:

Subject to the above, we do not have dissenting views on the remainder of the proposals in the consultation.