HM Treasury Consultation
Improving the effectiveness of of the Money Laundering Regulations

February 2024

Ordo response – 6 June 2024

Submission to: Anti-MoneyLaunderingBranch@hmtreasury.gov.uk by 9 June 2024

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 only.

*The information is only to be used by you in connection with the consideration of your response expanding variable recurring payments, 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 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 variable recurring payments (VRP).

Businesses can access the Ordo managed service in a number of ways: though an Ordo Merchant Acquirer/PSP payments partner, such as Access Group's Pay360 platform, directly via Ordo's business level APIs, and for smaller businesses, through 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 live with several clients for sweeping, but which require no further build or development to be rolled out for variable recurring payments beyond sweeping. Our platform allows 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, ensuring regulatory compliance and keeping up to date their own open banking customer journey.

Who's behind 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 launched its VRP service for sweeping clients in 2023. 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).

Summary

Through the work of the Payment Systems Regulator (the PSR) (being led by Head of Policy, Kate Fitzgerald) as part of the Joint Regulatory Oversight Committee (JROC), Government, regulators and industry have been collaborating to support and expand the roll out of innovative products and services within the open banking ecosystem. A key objective for all parties, and which the PSR is driving, is the launch of commercial variable recurring payments (VRPs) by Q3'24, which will provide greater choice and consumer control. Our response focuses on a potential perceived impediment to the successful rollout of VRPs this year which HM Treasury has an opportunity to address as part of its review of the Money Laundering Regulation (MLRs).

Under the MLRs, Payment Initiation Service Providers (PISPs) are required to conduct due diligence on their customer, so called customer due diligence (CDD) where they establish a business relationship with a customer. We have a business relationship with our customers, the merchants. Our client is either the payee, or a party providing broader technology platform services for many merchants of which our payment capability is a part. Either this technology platform provider facilitates its customers collecting money, or our merchant customer collects money, from their end-customers who are the senders of funds (the payers).

However, with the introduction of Variable Recurring Payments (VRPs), there is a risk some parties could interpret PISPs as establishing a business relationship with the payer. However, this is not the case. We do not have a business relationship with the payer. The payers agree with the merchant to sign up to a VRP mandate (like signing up to a subscription with Netflix or a direct debit with an energy company). The payer then authorises this mandate with their bank. The bank provides the PISP a copy of the authorised mandate, and we initiate payments in accordance with the mandate.

Any additional CDD on payers using VRPs will needlessly create friction in PISP payment journeys that is disproportionate to the level of money laundering and terrorist financing risk in the VRP product. It will prohibit VRP from being able to effectively compete with cards, a key PSR and HMT objective. It will also increase our operational burden, for no additional security benefits.

As with single payments, we believe requirements for PISPs to conduct CDD on the payer are:

- **Prohibited** - PISPs are prohibited from requesting, accessing, using or storing any information beyond that which is needed to provide payment initiation only, pursuant to regulation 69(3)(f) and (g) of the Payment Services Regulations 2017 and paragraph 17.65 of the FCA's Approach Document.

- **Duplicative** - the PISP initiating a payment from the payer's bank account, would be required to conduct CDD on the payer, despite the Account Servicing Payment Service Provider (ASPSP) already having performed CDD on the payer.

- **Unnecessary and disruptive** - PISPs do not hold or transmit any funds themselves. They instruct ASPSPs to move money at the account holders' request between PSD2 compliant ASPSPs. As such they are very low risk of money laundering. In addition, PISPs will have to gather additional data to perform CDD on payers, which will create friction in the payment journey and could increase failure rates and decrease conversion.

- **Unequal** - providers of comparable products (e.g. cards and direct debit) are not required to perform such checks on payers.

Our proposed solution is that HM Treasury updates the MLRs so that it is unambiguously clear that a PISP's customer is the merchant, not the payer. This would ensure the UK keeps pace with the EU, which introduced this clarification as part of the recently adopted EU AMLRs.

Making this change to primary legislation would provide the greatest clarity and certainty to industry. However, in light of JROC's (and the Government's) desire to see commercial VRPs launched and adopted by UK merchants via a Phase 1 rollout by Q3'24, we believe it would also be appropriate to update anti-money laundering (AML) guidance to industry provided by the Joint Money Laundering Steering Group (JMLSG). This would be a quicker way of addressing the issue and serve to bridge the gap until such time as the MLRs are amended.

Why money laundering and terrorist financing risks are limited for PISPs and VRPs

Our role as a PISP is limited to initiating payment instructions to ASPSPs on behalf of the customer. The money laundering and terrorist financing risks are therefore not increased by the use of a PISP as compared with the payer submitting the payment order themselves.

A PISP initiates a payment directly from an account held by a payer with a regulated ASPSP who will have already verified the identity of the payer by applying CDD measures upon opening the payment account. Because there is an underlying customer relationship between the payer and the ASPSP, there is no need for PISPs to duplicate the checks with a party with whom the PISP does not have a relationship and about whom they are not permitted to gather information.

Finally, PIS is a more secure payment method than direct debit. This is because the payer undergoes strong customer authentication (SCA) at their bank prior to a payment being initiated under a payment instruction / mandate. The payer must prove that they own the bank account on which the VRP mandate is set up before the mandate is established and the PISP initiates the payment orders.

Impacts of the application of the MLRs to PISPs

1. Prohibited from collecting information

Payment Initiation Services (PIS) are a product of PSD2 and use modern secure technology. They are also a post-General Data Protection Regulation (GDPR) innovation and therefore have been built in compliance with the GDPR principle of privacy by design. This reflects the legislative and regulatory framework that directly governs PISPs. Regulation 69(3)(f) and (g) of the Payment Services Regulations 2017 specifically restricts what information PISPs can collect and what they can do with that information - provide a payment initiation service only. This is repeated in the FCA's Approach Document at paragraph 17.65.

2. Duplication makes it a redundant process

Performing CDD on payers would require PISPs to add checks that already exist within the payment chain. This is because a payer's primary relationship is with the ASPSP, and they also have a significant relationship with the merchant. The ASPSP is already under an obligation to carry out AML and counter-terrorist financing (CTF) checks on their customers when opening an account for them, and the ASPSP will also be monitoring the transactions initiated by the PISP. Where items are of a high value, certain merchants, such as estate/letting agents, car dealers etc, will also be carrying out AML checks. Any CDD checks performed on payers by PISPs when initiating transactions are therefore duplicative and do not add any value or work to mitigate any residual risk.

3. Unnecessary friction to customer journey

The duplicate checks require PISPs to add additional steps to the payer's customer journey. At a minimum, PISPs would need to collect the payer's identification information, which include their name, address, and date of birth. The details collected from payers (e.g. name, DOB and address) then need to be verified to ensure that they are who they say they are.

This would add unnecessary friction to open banking payment journeys and would lead to a significant drop in conversion rates. This would prohibit VRPs from being able to compete with cards and banks, a key regulatory and government objective (more detail below).

4. Unequal to comparable products

A primary objective of the Payment Services Regulations, CMA Retail Banking Order and the Payment Systems Regulator itself (as well as Government policy on retail payments more generally) is to increase innovation and fair competition by providing consumers with more choice and options. Requiring PISPs to gather this data and perform these checks within the scope of the MLRs is counterproductive to this purpose because it requires PISPs to comply with stricter requirements in comparison to competitors with similar business models, such as merchant acquirers and the setting up of direct debits. This will not only require

PISPs to incur increased compliance costs, but it will also cause payer dissatisfaction (and in some cases confusion), which will ultimately lead to increased transaction abandonment during the PISP process.

Entities such as merchant acquirers do not perform these checks on payers at the checkout, and neither does a payee's bank undergo such CDD when a direct debit is set up by a payer. In both cases, unlike PISPs, the merchant acquirers and recipient bank are also in possession of funds. Requiring PISPs to carry out these checks on payers leads to friction which means that they are not on a level playing field with more traditional payment services.

A PISP does not provide a potential money launderer or terrorist financer with any capabilities that would make laundering money or financing terrorism any easier than, for instance, using the card network, Faster Payments, or Direct Debit. In fact, PISPs rely upon authentication procedures set by the ASPSP during the payment flow, so are at lower risk of being used to commit money laundering or terrorist financing.

The PISP's customer

PISPs are subject to the MLRs as they fall within the definition of "Financial Institutions". The starting point for Financial Institutions, including PISPs, is to determine who is their customer. This is largely determined by reference to "business relationship" as defined by Article 3(13) of the Anti-Money Laundering Directive, which means a *"business, professional or commercial relationship between a relevant person and a customer, which:*

a) arises out of the business of the relevant person, and

b) is expected by the relevant person, at the time when contact is established, to have an element of duration."

In a direct merchant-facing PISP model, it is the payee who is the direct customer of the PISP rather than each individual payer. This is highlighted by how a payer may interact with a merchant-facing PISP, where typically the payer:

a. cannot use the PIS independently of paying the payee that has contracted with the PISP to offer PIS as a payment method;

b. can only use the PISP to initiate payments to the specific payee, with whom the end user has a relationship that has contracted with the PISP (i.e. it cannot freely make payments to any payee of its choice);

c. does not have an account with the PISP; and

d. does not pay the PISP any payment transaction fees.

The above issues have already been addressed by the European Union. In the recently finalised text of the EU Anti-Money Laundering Regulation (AMLR), recital 62 notes:

> *Some business models are based on the obliged entity having a business relationship with a merchant for offering payment initiation services through which the merchant gets paid for the provision of goods or services, and not with the merchant's customer, who authorises the payment initiation service to initiate a single or one-off transaction to the merchant. In such a business model, the obliged entity's customer for the purpose of AML/CFT rules is the merchant, and not the merchant's customer. Therefore,* ***with respect to payment initiation services, customer due diligence obligations should be applied by the obliged entity vis-a-vis the merchant.*** *In relation to other financial services that fall within the scope of this Regulation, including where provided by the same operators, the determination of the customer should be done having regard to the services provided.*

The EU's approach offers a helpful insight into how the UK could address the issue.

Proposed solution

Ensuring CDD on payers is not required for PISP-initiated payments will level the playing field, facilitate choice and innovation in the payments market (specifically VRPs), and help the UK to maintain its competitive advantage in open banking.

Ordo recommends that HM Treasury updates the MLRs to clarify that PISPs do not have to conduct CDD on payers. This would offer the most long term certainty to firms in the open banking ecosystem, notably PISPs.

However, we recognise that amending primary legislation can be a time consuming process. In light of JROC's (and the Government's) desire to see commercial VRPs launched and adopted by UK merchants by Q3'24, we believe it would also be appropriate to update AML guidance to industry provided by the Joint Money Laundering Steering Group (JMLSG). This would be a quicker way of addressing the issue and serve to bridge the gap until such time as the MLRs are amended.

JMLSG issues guidance to firms and their staff in relation to the prevention of money laundering and terrorist financing, and allows them some discretion as to how they apply the requirements of the UK AML / CTF regime in the particular circumstances of the firm, and its products, services, transactions and customers.

JMLSG's "*Guidance for the UK Financial Sector - Prevention of money laundering / combating terrorist financing*" ("**Guidance**") could be updated by adding PIS as a new sector to "*Part II: Sectoral Guidance*". The

updated Guidance should exempt PISPs applying CDD on the payer whenever the PISP initiates any transaction (i.e. single or one-off transactions, as well as recurring transactions) to the respective payee, in situations where the payer does not use the PISP independently of paying that payee.

There is a precedent for this approach: prior to the EU concluding discussions on the AMLR, the European Banking Authority published Guideline 18.8 of the Sector Guidelines on AML Risk Factors. This says:

> *"In the specific case where the PISP has a business relationship in the meaning of Article 3(13) of Directive (EU) 2015/849 with the payee for offering payment initiation services, and not with the payer, and the payer uses the respective PISP to initiate a single or one-off transaction to the respective payee,* ***the PISPs' customer for the purpose of these Guidelines is the payee, and not the payer****."*

It would be helpful if this is adopted by JMLSG for single and repeated payments in the UK, whilst awaiting amendment of the MLRs for full clarity and certainty. By taking forward these two recommendations, HMT will be supporting the roll-out of a cheaper, safer, more customer-centric payment proposition than is currently available to merchants and consumers.

If you would like to discuss any point, please do not hesitate to get in touch.

All the best

Fliss Berridge
Director & Co-founder