Authorised push payment (APP) scams: Requiring reimbursement

Open Finance Association (OFA) response to the Payment Systems Regulator (PSR)

About the Open Finance Association (OFA)

The OFA represents companies focused on empowering consumers and businesses to access account data and make safe and secure payments through open APIs (application programming interfaces). We represent the open finance providers and users of open finance. Our members include:

- Armalytix
- Crezco
- Nuapay
- FinAPI
- GoCardless
- Ordo
- Plaid
- Token
- TrueLayer
- Volt
- Worldpay
- Worldline
- Yapily

Summary

We welcome the opportunity to respond to the PSR's consultation on APP scams. APP scams can have a devastating impact on victims' lives and we recognise the urgent need to tackle the issue. OFA is fully supportive of the drivers to provide an appropriate level of consumer protection. However, as the consultation paper focuses on liability between banks, we have not responded to individual questions but instead highlighted areas for further consideration by the PSR.

We believe that the adoption of open banking payments by business and consumers will itself be an effective countermeasure to APP scams because open banking payments tackle the root causes of APP scams inherent in manual bank transfers.

However, we also believe the PSR's APP scam proposals, as they are currently formulated, put the viability of open banking at risk for the following reasons:

- **De-risking:** Open banking companies already struggle with banks limiting and blocking legitimate open banking payments. Imposing further liability on banks will reduce banks' risk appetites, leading to further limiting and blocking of legitimate open banking payments, and make open banking untenable as a payment option (removing a potential competitor to cards).

- **User experience** - even 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.

- **Cost of faster payments** - It is likely that the proposed APP scam measures will increase costs for sending and receiving banks (e.g. costs of managing disputes and FOS escalations). These will be passed onto merchants in the form of charges for receiving faster payments. This will make open banking an unattractive option for merchants, because the costs to receive faster payments via open banking will be greater than the cost to receive card payments.

We do not think that there has been sufficient consideration of these impacts of the APP scam proposals on open banking payments, evidenced by the fact that the only reference to payment initiation services in the consultation is a single, undefined footnote at section 4.6.

The PSR has rightly recognised that open banking has *"the clear potential to facilitate account-to-account payments for retail transactions and compete with card systems."*[1] Without further consideration, for the reasons set out above, OFA are concerned the PSR's APP scam proposals present a significant risk to this potential and to the PSR realising its objectives in this space.

Proposals:

Before the PSR implements any final rules, the OFA would ask it to:

1. Explicitly recognise the security benefits of open banking payments and **consider how to support the adoption of open banking payments as an alternative to manual bank transfers and as a countermeasure to APP fraud**.

2. **Conduct a separate cost benefit analysis of its APP scam proposals in light of the impact they could have on open banking payments**, and the detrimental downstream impact this could have on the PSR's work to promote competition from A2ART for card payments.

3. **Delay the implementation of any changes to liability until more data has been collected on whether existing APP scam measures (CoP and CRM) are working.**
    - We note that the latest UK Finance half-year APP fraud statistics (H1'22) showed — for the first time — a significant year-on-year reduction in APP fraud in both volume (-6%) and value (-17%) terms. Although undoubtedly still high in absolute terms, directionally this suggests that existing measures are beginning to have an impact on APP fraud and more time is required to assess their full impact.

[1] https://www.psr.org.uk/our-work/account-to-account-payments/

4. **Consider whether measures are necessary to ensure banks take liability for blocking legitimate PISP-initiated payments - and compensating end users appropriately - unless they are able to provide clear evidence for the decision.**
    - At the moment, banks carry no burden of proof for declining transactions of any nature and are under no obligation to explain their action even when challenged with specific evidence supporting the legitimacy of a payment. However, consumers may incur financial damage by a payment not completing, for example if they miss a deadline (such as HMRC's tax return deadline). We believe consumers should be compensated in situations when they experience a materially adverse financial impact from a payment not completing (i.e. it should not be compensation purely for the inconvenience caused).

In addition, we note the proposal at section 6.7 of the consultation indicating the PSR's expectation that Pay.UK will *'establish, maintain and enforce cross-market arrangements on PSPs' conduct in a number of areas, including as part of its role in assessing and enabling use cases for the NPA, such as open banking account-to-account retail transactions.'*

5. More clarity is needed from the PSR on what is meant by this, and how it interplays with discussions under the Joint Regulatory Oversight Committee (JROC) to develop a future entity to oversee open banking standards. **The Open Finance Association strongly believes that standards relating to open banking providers should be the responsibility of the future open banking entity, not Pay.UK.**

The OFA recently responded to the Strategic Working Group (SWG) process informing JROC's work on the future of Open Banking in the UK. We believe one of the recommendations we made in that process could be relevant to assisting with mitigating APP scams:

6. **We recommend that the Open Banking Implementation Entity (OBIE) or successor entity coordinate the mandatory implementation of transaction risk indicators (TRIs) so that receiving institutions can use them to assist risk-based decisions in a meaningful way.**

<u>Further detail</u>

Why open banking payments can counteract APP fraud

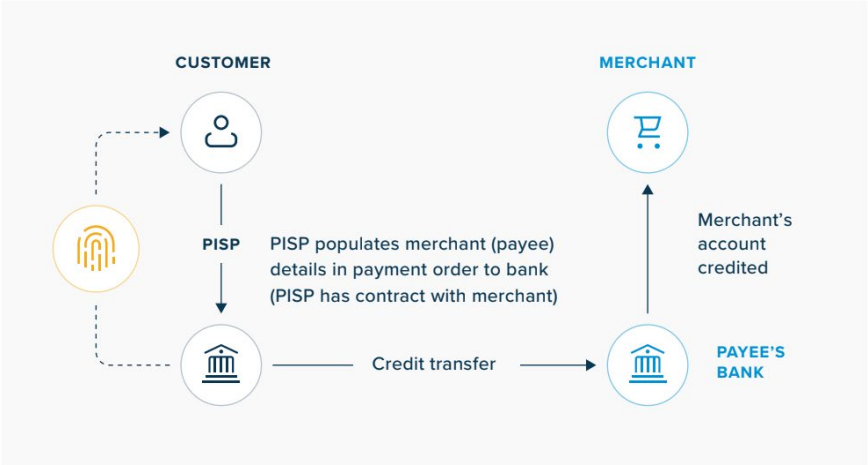
Open Banking payments to merchants are an inherently safer way to pay than other forms of payment, especially manual bank transfers, which are the main vector for APP scams. The way open banking payments are set-up addresses the risks of APP fraud because:

- **Open banking providers onboard and carry out due diligence with the payee** - When an open banking provider enables payments for a business, they enter into an ongoing commercial contract with that business, and undertake due diligence on the business as part of that. This reduces the likelihood that the beneficiary of an open banking payment will be used for fraud. In the unlikely event that fraud occurs, the open banking provider can immediately raise this with their client (the beneficiary).

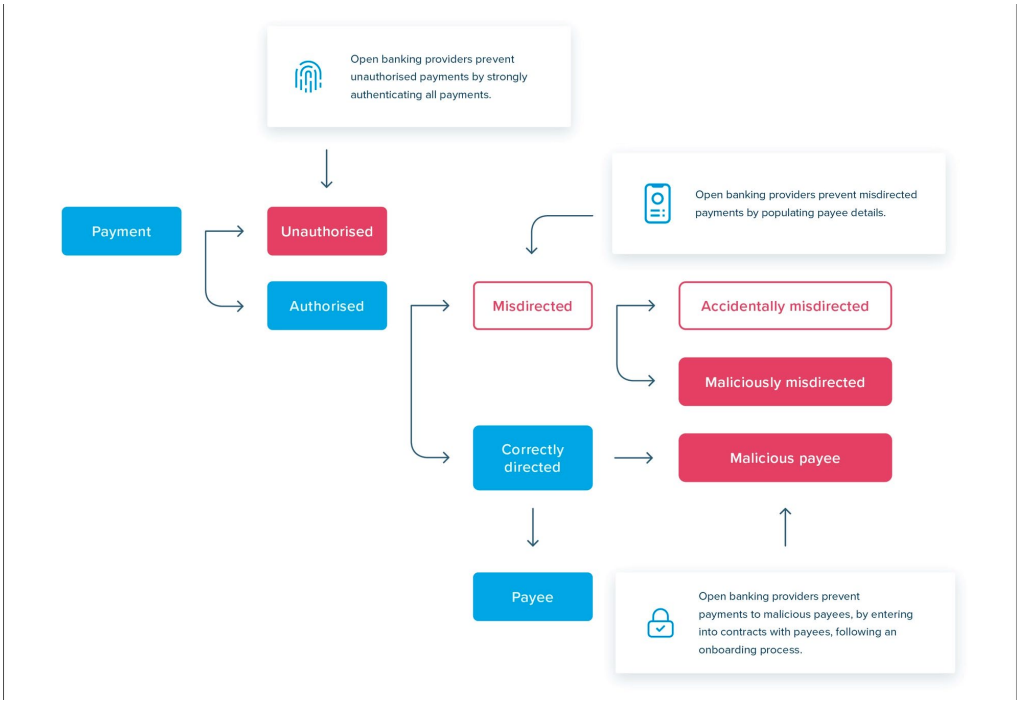
- **Payee details (sort code and account number) are pre-populated by the open banking provider, removing the possibility of human error** when typing payee details or customers being tricked into sending money to an account controlled by a fraudster. The beneficiary's name is also presented back to the payer by the payer's banks in the authentication journey.

Fig. 3

Open banking payment to merchant: open banking provider populates the merchant's account details



How open banking prevents fraud (including APP fraud):



This is why the Open Banking Implementation Entity (OBIE) noted last year that, *"the risk of APP fraud in Merchant Initiation via PISP is* ***exceptionally low****"*[2] (emphasis added).

[2] Open Banking, *A2(d) - Open Banking Standards Relating to Confirmation of Payee and Contingent Reimbursement Model Code: Consultation Document*, 2021

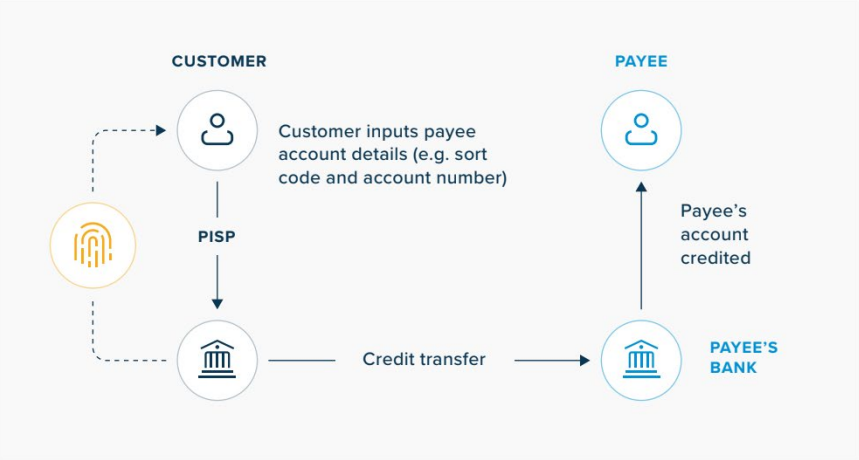
Indeed, OFA believes that as open banking payments replace manual bank transfers in day-to-day life, APP fraud will continue to decrease and customers will start to see manual bank transfers as less convenient and less secure. In short, customer uptake of open banking will further reduce the risk of customers being involved in APP scams.

Do all open banking payments reduce the risk of APP fraud?

Open banking payments can be used in a similar way to manual bank transfers in what are known as 'party-to-party' use cases. In this use case, the consumer (rather than the PISP) populates the payee details which means they could potentially be manipulated into entering the wrong details. However, this use case is increasingly rare (Yolt Pay enabled this, with Yolt Pay, but has since closed down).

Fig. 2

Open banking payment where consumer inputs recipient details



How does a bank know if an open banking payment is low risk of APP fraud or not?

Parties across the open banking ecosystem already apply a risk-based approach to open banking payments. For example, banks in monitoring transactions for high risk factors, and TPPs conducting due diligence on the businesses they offer services to.

There are, however, changes in open banking standards that could be made that would enhance the risk-based approaches applied by open banking ecosystem players.

Current OBIE standards enable PISPs to send 'payment context codes' (PCCs) to banks, which allows them to understand the risk profile of a payment. For example, a PISP can tag a payment with an 'Ecommerce' code if the payment is to a merchant, or 'party-to-party' if the consumer is using the PISP to make a payment to another account of their choosing, such as paying a friend.

The latest version of the OBIE standard (3.1.10) has introduced more detailed transaction risk indicators (TRIs), which are supposed to give banks further information about the risk profile of payments, e.g.:

- **ContractPresentIndicator** - Indicates if the Payee has a contractual relationship with the PISP (the thinking being that if a PISP has a contract with the beneficiary they will have undertaken due diligence, lowering the risk of any payments to the beneficiary).

- **BeneficiaryPrepopulatedIndicator** - Indicates if a PISP has immutably pre-populated payment details in for the PSU (the thinking being that if a PISP rather than the consumer has populated the payee details, the payment will not be vulnerable to APP fraud).

However, the implementation of these TRIs and PCCs is voluntary and is not being coordinated by the OBIE, leading to inconsistent and patchy implementation by both PISPs and banks. It risks the benefits of payment risk information not being realised and a continuation of arbitrary risk management by banks, leading to more PISP transactions being limited or blocked unnecessarily.

We recommend that the OBIE or future entity coordinate the mandatory implementation of TRIs so that receiving institutions can use them to assist risk-based decisions in a meaningful way.

De-risking

It is important to highlight the implications the PSR's proposals for APP reimbursement may have on the development and adoption of Account to Account (A2A) Retail Transactions.

The PSR believe that A2A payments will increase choice for merchants and consumers and give an additional option for both POS and e-commerce transactions, however if the proposals for APP reimbursement were to set the benchmark for A2A this could significantly damage this proposed new payment option.

A 'reimburse first, investigate later' culture applied to A2A payments may mean that banks build such a robust and defensive economic model around them that they are unlikely to be economically appealing as a payment method. In open banking, this could manifest itself by banks blocking and limiting transactions initiated by PISPs to payees they perceive to be in higher risk sectors.

There is already evidence that banks are de-risking in the way that they are blocking payments for entire sectors. The payments sector has faced substantial derisking already in the remittance sector and this 'reimburse first, investigate later' approach will disproportionately impact another cohort of firms authorised under the Payment Services Regulations.

User friction

We believe that the current proposals are likely to incentivise banks to introduce additional friction in instant payment journeys, such as more screens, 'pop up' warnings and/or verification steps for consumers when authenticating payments. This will damage the payer experience and reduce trust in Open Banking overall. The OBIE concluded last year for PISP-initiated payments, *"[Confirmation of Payee and Contingent Reimbursement Model pop up] warning messages are of limited utility and that the resultant additional friction together with*

the incremental costs of deployment are not justified. Indeed, emerging evidence from our consumer research suggests that there would be positive benefits from eliminating the overuse of warning interventions; customer fatigue erodes their effectiveness."[3]

OFA members also believe there will be an increased propensity for banks to suspend payments for fraud checks and look to generally slow down the payment process. One approach for achieving this we are aware is being discussed is to introduce delays in high value faster payments transactions so that banks have more time to scrutinise payments. Whilst we are fully supportive of appropriate measures to mitigate fraud we are concerned that unnecessary and indiscriminate application of such friction will have a significant negative impact on open banking payment propositions.

It is also contrary to the direction of travel abroad; other jurisdictions are looking to introduce real-time payments rails because of the benefits to the economy they bring. For example, the EU Commission recently proposed a new Instant Payments Regulation with the intention of creating a system that can compete with the UK's Faster Payments System. Reducing the speed with which payments are settled via FPS could impact the UK's perceived and actual international competitiveness.

Cost of faster payments

Changing the liability model for reimbursing APP scam losses may prompt ASPSPs to revisit the economic model they use for instant payments and e.g. increase charges to businesses for instant payments, or even consider introducing charges to consumers for sending or receiving Faster Payments.

Businesses are typically charged by their banks to receive Faster Payments into their bank account, with fees varying significantly and typically being lower for larger businesses (for example, one CMA9 bank offers tariffs charging £0.35 per incoming payment for businesses <£5m turnover and £0.15 for larger businesses). By comparison, when using card payments, low value transactions are typically charged on an ad valorem basis (i.e. percentage of transaction value). The BRC recently reported that merchants on average pay 26bps of turnover to accept debit cards (small merchants can pay significantly more than this). On an absolute basis this amounts to ~3p for a £10 sale.

This means that open banking payments are already uncompetitive with card payments at low values. The APP liability shifts could further exacerbate this problem and prevent open banking A2A payments from being a competitive constraint on card payments.

If you wish to discuss the OFA's response please do not hesitate to contact openfinanceassociation@fticonsulting.com.

[3] Ibid