

10 September 2021

**PSR Strategy
Payment Systems Regulator
12 Endeavour Square
London
E20 1JN**

To: psrstrategy@psr.org.uk

Cc:

FDATA Response to PSR Consultation paper on PSR Proposed Strategy June 2021

Dear PSR Strategy Team,

We appreciate the opportunity to feedback on the PSR proposed five-year strategy plan, which is detailed below.

Yours faithfully,

Ghela Boskovich
Regional Director, Head of Europe
Financial Data & Technology Association

FDATA Feedback:

The principles of competition, security, reliability, fair access, innovation, and regulatory alignment that comprise the strategy are principles we strongly support. The four priorities, as outlined in the strategy document, FDATA and its members also strongly support.

Our feedback specifically addresses how this looks like in practice; we would like to remind the PSR of the principle of proportionality, as well as preserving space for the industry to creatively and innovatively respond with solutions, in developing consumer protections associated with interbank – or open banking – payments.

The TPP community has every incentive to ensure consumers' payments are protected, and that their experience in using interbank payments is smooth, safe, and secure. PISPs are in position to serve both retail end consumers and merchants/SMEs, and are the first port of call in the open banking payment customer journey. PSD2 also provides clear and explicit guidance

on who makes the customer whole when a payment goes wrong. Purchase protection liability has also been clearly detailed in the Consumer Right Act of 2015: the merchant is liable if the good or service is faulty.

The PSR and OBIE work on consumer protections acknowledges this; however, the discussion has expanded to include purchase protection, and what liability a TPP assumes for a bad purchase. The discussion has evolved to conflate payment protection with purchase protection, and we urge the PSR to tread cautiously here, as a balance needs to be struck that allows open banking payments to properly compete with cards, but not incur the same operational costs or purchase protection features (such as chargebacks) associated with the card schemes.

Interbank/open banking payments are meant to be a competitive alternative to cards; as such, they are not the same thing as a card payment, they should not identically match as they are fundamentally a different type of payment, processed on a different system, with a different operational flow, differing set of counterparties, and a different set of risks.

The hypothesis that purchase protection needs to happen now, before the starting pistol has even been fired, is a fragile one. This question actually requires more data, more consultation, more direct PISP feedback, and more use case review.

Purchase risk has always existed; it is simply the process associated with deciding on handing over money for a good or service. Cash, for example, has zero purchase protection. Irrespective of how one chooses to pay, there is always a purchase risk: cash, cheque, direct debit, credit card, and now open banking payments. Each payment instrument has a different level of purchase risk. It is crucial to remember the rationale for why the protections were adopted before assuming that purchase protection pre-baked into the payment instrument is necessary. Section 75 of the Consumer Credit Act 1974 was introduced to protect people against the risk of opening a line of credit. Card chargeback was introduced to manage the extremely high levels of fraud in the card schemes. Chargebacks were designed to protect the *effective operations of the schemes*, not consumers. Any consumer purchase protection is a positive externality not included in the original intent.

Not all payments need to have the exact same purchase protection.

By contrast, PISP for purchases are not vulnerable to scams or fraud, because the PISP has a contract with the merchant, and the payment instruction is initiated at the point of sale. The discussion of Authorised Push Payment fraud scams in relation to open banking payments is limited to peer-to-peer, where the consumer is populating the instruction. By contrast, the merchant's PIS provider is populating the bank details, at the point of a genuine transaction. There is no chance of scam in a merchant-initiated payment scenario. This is a key conflation that continues to negatively shade the discussion on appropriate levels of consumer protection.

Moreover, APP fraud warnings are meaningless in a purchase scenario. Since the PISP has a contract with the merchant, there is no need to ask the customer if they're sure they want to pay the merchant. The customer knows they are paying the merchant, and there is no way the customer can pay anyone else, since the PISP populates the payee details. Payee account data is provided by the merchant, so there is no risk of incorrect data being entered.

For the vast majority of open banking payments – outside of the peer-to-peer or me-to-me use cases – merchants will be the primary initiators. And the merchant is already liable for purchase protection. There are also mitigants that reduce the risk of merchants as bad actors.

PISPs have every incentive for good customer outcomes, and much of that revolves around pre-emptive actions *before* a payment is even initiated. And since open banking providers have more control of who they serve, and can take additional steps to prevent the likelihood of purchase disputes as well as assist when things go wrong:

- Rigorous onboarding of merchants – ensuring that merchants who offer open banking payments have a track record of processing refunds and dealing with purchase disputes; no PISP wants to work with a disreputable merchant
- Contractual agreements with merchants – setting out the expectations and process of customer purchase dispute resolution
- Process to handle customer queries – PISPs and merchants' customer care teams can work together to quickly deal with purchase issues

In an open banking payment purchase, there are just three actors, who all have relationships with each other, so purchase issue resolution can be rapid, in contrast to card schemes, which have lots of counterparties. It is the counterparty complexity that makes chargeback resolution very slow and very expensive.

Since these mitigants already exist, it begs the question of whether or not some of the specific purchase protection risks are real or hypothetical, and whether or not these efforts are aimed at solving an actual problem or a hypothetical one.

While interbank payments may be new to the UK market, other markets – especially Europe – have two decades of experience. The experience and evidence point to the fact that both fraud and purchase risk are minimal compared to cards and can be handled without any card-style chargeback mechanism. Any attempt to create chargeback purchase protection parity for interbank payments dismisses the technological improvements in security, design, and operational efficiencies by introducing unnecessary overhead and cost, thus rendering them a less attractive alternative to cards. This negates, erases even, the principle of competition in payments.

Even in the case of high value transactions, the market is already pushing for direct bank payments, especially outside of the UK, without additional purchase protections being

mandated by other EU state regulators. In some cases, purchase *insurance* is offered, but it is not integrated into the features of the electronic payment itself.

Instead, refund functionality would have a more positive impact on making open banking payments more competitive with cards. At the moment only a few ASPSPs in the market provide that functionality; to fulfill its strategy, the PSR would be better served to encourage refund capability across the market.

Again, we point to the fact that not all payments need to have the exact same level of protection.

The PSR's five year strategy is solid, and reflects an evolutionary approach to the changing nature of how payments in the UK will be delivered. FDATA sees the merit and strength of such an approach. We also recognise that the current conversation around appropriate consumer protections requires an evolution: conflation of two different objectives and the liability assigned to actors in the value chain needs resolution, as does the assumption of the validity of the hypothesis require further examination, and the hypothesis itself requires iteration.

FDATA urges caution when handling the exam question of purchase protection in open banking payments. Mishandling of this issue will kill open banking payments, failing to deliver a viable competitive alternative to card payments, at the significant tangible economic cost to merchants and small businesses across the UK, and at a significant opportunity cost to all those actors in the value chain from retail consumers to ecommerce firms to PISPs and banks alike.