HM Treasury's

Payments Services Regulations: Review and Call for Evidence

6 April 2023

Ordo response

Submission by email only to PaymentServicesCfE@hmtreasury.gov.uk

The following information is the property of The Smart Request Company Ltd, trading as Ordo and is provided to you in response to the above Call for Evidence only.

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 turn-key service in a number of ways: though an Ordo Merchant Acquirer/PSP payments partner, such as Access Group/Pay360, 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 hosted and 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. Ordo services plug and play solutions so businesses can be up and running and saving from day 1.

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.

Ordo welcomes the opportunity to provide input on HM Treasury's (HMT) call for evidence (CfE) on its review of the Payment Service Regulations (PSRs).

The PSRs, combined with the CMA's open banking order, have been the key regulatory enablers of open banking in the UK to date. However, the regulatory framework for Open Banking in the UK is now undergoing a period of fundamental change and uncertainty, including:

- HMT's review of the PSRs, the foundational regulation that both enables and governs the provision of open banking in the UK and the players in the ecosystem (although we note that in the CfE, HMT states that "[i]n sum, the government is progressing the further development of Open Banking outside the scope of this review."[1]);
- the implementation of the CMA's open banking order coming to "substantive completion";
- the imminent Joint Regulatory Oversight Committee (JROC) report on the vision for the future of Open Banking and recommendations on the design of the future Open Banking entity; and
- the recently laid Data Protection and Digital Information (No. 2) (DPDI2) bill which contains provisions for a "Smart Data" framework that could in due course form the basis of the long-term regulatory framework for Open Banking.

These simultaneously live initiatives with multiple policy decision-makers need to be read and considered holistically, and especially the imminent JROC report once published, given its potential significant impact on the open banking regulatory environment, and on which we have commented on multiple occasions.

Ordo would ask that HMT takes this into account when considering responses to its CfE with respect to open banking. We may make an additional submission after HMT's deadline of 7 April following consideration of the JROC report once published.

Our response to the CfE is structured as follows:

i. **Amend ASPSP obligations to enable open banking and the TPPs that deliver open banking services to effectively grow, compete with ASPSPs existing services and innovate**: Our views on changes to the obligations placed on ASPSPs that are required to enable open banking TPPs to effectively grow, compete with ASPSPs existing services and innovate.

ii. **Evolving the broader regulatory framework to support open banking**: Our views on issues in the broader regulatory framework that should be considered as part of the HMT review.

iii. **Emerging fraud threats and open banking**: Our views on emerging fraud threats and related policy initiatives with respect to their impacts on open banking.

[1] HMT CfE, para 58.

i. Amend ASPSP obligations to enable open banking to effectively grow, compete and innovate

Relevant consultation questions:

1. How should the payment services framework evolve – and what should be the government's priorities – to better promote the following government objectives for payments regulation:
   - A. Achieving agile and proportionate regulation, which facilitates the international competitiveness of the UK economy through growth and innovation in the UK payments sector
   - B. Ensuring appropriate trust and protection for consumers
   - C. Ensuring the resilience and integrity of the UK's payment market
   - D. Fostering competition, in the interests of consumers

   8. Does the regulatory framework for payment initiation service providers (PISPs) and account information service providers (AISPs) sufficiently support the growth of this sector, and ensure a level playing field, and fair access to payment accounts, to support competition and growth?

   18. Does the existing framework strike an appropriate balance of rights and obligations between: Sending and receiving payment service providers? Account servicing payment service providers and payment initiation service providers/account information service providers?

To deliver the objectives of more competition and innovation in payments, user adoption of open banking is key. But users will only adopt open banking if it's widely available, addresses their key needs, is trusted and delivers a consistently good experience. Ordo has identified critical points where changes to the obligations placed upon ASPSPs are essential to deliver on these outcomes. It is vital to note that new and innovative payment services from open banking for UK businesses and their consumers will be provided by TPPs. And that these new services will almost universally be competing with existing and mature services from banks and card companies (for whom much of the profit created goes to banks via card issuing fees). Existing card services generate substantial oligopolistic profits for banks. If TPP open banking innovation is to compete with these services, delivering enhanced value to businesses and consumers, bank's overall revenues from a combination of cards and open banking must be reduced. Therefore, any further enablement of open banking by ASPSPs (the same banks making money from cards today) will cannibalise their revenues. This means that there is no business case for ASPSPs to enhance competition to themselves voluntarily via open banking and that regulatory interventions to enable open banking will be needed to allow open banking payments competition to cards (and the banks that receive a significant proportion of card profit through issuing fees) to be effective.

Increase and standardise transaction limits across ASPSPs

Different banks impose different limits on transactions: some stop open banking transactions as a first payment of any amount (meaning an open banking payment can only be executed if a first payment to the payee had already been done with direct bank payment, undermining the open banking use case), significant numbers of open banking payments in the sum of ≥£1,500 are blocked altogether, and some block both. If this is permitted to continue, it will severely impact the competitiveness and viability of open banking payments in the UK.

These differing levels also mean that some open banking use cases may be prevented for certain PSUs but not others – these uncertain and apparently random restrictions destroy merchant trust in open banking payments. As part of the baseline, there needs to be consistency in the amounts that PISPs can initiate across banks so that customers and their merchants receive a consistent experience.

Furthermore, ASPSPs must be required to justify the stopping of any payments for fraud reasons, and stop payments only as a last resort after having implemented other more effective and accurate fraud prevention measures. This needs to be monitored and enforced, must be applicable to all ASPSPs to be implemented consistently, and across ASPSPs and channels.

Please see fraud section below and the suggestion that the receiving bank ringfence funds in the event of suspicion, resulting in stopping fraud *not* payments. Early and proper implementation of Transaction Risk Indicators (TRIs) by ASPSPs would allow TPPs to confirm to an ASPSP that the payee in a transaction has been validated by the TPP as a legitimate payee meaning that holding of the payment by an ASPSP due to Authorised Push Payment (APP) scam concerns could be completely avoided for these payments. This

change would allow TPP services to play a much more substantial role in using their capabilities to provide APP scam free payments services, and would lower ASPSP fraud avoidance costs.

Widen mandatory implementation of the Open Banking standards to beyond CMA9 and progress non-sweeping VRP

To date, implementation of the Open Banking Implementation Entity's standards and guidelines has only been mandated for the CMA9, leaving all other ASPSPs more flexibility in how they implement the related open banking requirements placed on them under the PSRs.

Whilst this has gone some way to enabling consumers and businesses to access open banking, many are still being excluded because their bank is not participating. Lack of coverage, meaning incomplete coverage, makes it harder for FinTechs to justify to businesses the costs of integrating open banking solutions. We see this particularly with new Open Banking innovations like VRP, where rollouts beyond the CMA9 are lagging behind.

As such, the Open Banking mandate should be extended to cover a significantly wider set of ASPSPs for CMA order functionality.

The CMA order functionality boundaries, particularly for VRP also need to be broadened substantially and quickly if open banking payments are to succeed in driving competition and innovation.

The CMA6GB have built, paid for, and deployed full VRP services, which they are limiting to the sweeping use-case. TPPs and their customers can see huge opportunities to use VRP to enable a whole host of valuable new services that can compete with cards and Direct Debits, both in terms of costs and importantly functionality.

Having required banks to build VRP the CMA Order has limited VRP usage to sweeping use cases because of legitimate concerns about consumer protection from malicious billers in other situations. Note, this is not a use case concern, but a biller concern. Given this, a significant portion of the future economic potential of VRP could be enabled, without consumer protection concerns, by enabling mandated VRP for properly regulated industry sectors. Sectors where comprehensive legislative and regulatory protection for consumers already exists, namely business regulated by, for example: The FCA, Ofgem, Ofwat, Ofcom as well as central and local government departments and agencies, and Charities. Application in these areas could provide businesses with new opportunities to help support the cost-of-living crisis. As well as opening up this market, the sector-based biller restriction is easy to define and police, unlike sweeping use case restrictions which remain difficult to pin down precisely, giving ASPSPs opportunities to thwart even currently permitted usage.

The additional costs to ASPSPs of supporting this broader application will be very low, the development of VRP has already been done, and the economic benefits to businesses and their customers from VRP will be substantial, making a strong case for intervention.

But it remains true that due to the pro-competition cannibalisation of card issuing revenues for banks this will entail, they will not support expansion of VRPs voluntarily, or at least not unless they can charge TPPs new fees to offset their card revenue losses, undermining the competitive benefits of VRPs. Such an operating cost recovery model where ASPSPs charge TPPs for VRPs is untenable because ASPSPs will try and avoid cannibalisation and there are no market forces acting on their pricing as each ASPSP is a de facto monopoly provider of VRP services for its own customers. In engagements with ASPSPs re non-sweeping VRP, the ASPSPs have been explicit in stating that they are either pricing this to prevent cannibalisation of card revenues or will not offer non-sweeping VRP because of the risk of cannibalisation.

However, the existing single payment and sweeping ASPSP charging model means that ASPSPs will be paid for the underlying Faster Payments used to deliver VRPs, covering their operating costs, while still allowing competition between banks to set a proper market price. Therefore, ASPSPs will need to be mandated to use this existing open banking payments charging model for non-sweeping VRPs and not entertain an undeliverable and unnecessary premium API charging idea.

It should be noted that unlike Account Information Services (AIS), banks are being paid for Payment Initiation Services (PIS) by their customers through the underlying Faster Payment charges.

Looking at this in more detail, there are two key factors in extending VRP beyond sweeping: ASPSP charges, and a managed roll out across sectors.

ASPSP charges

It is imperative ASPSP charges are addressed by the regulator as an immediate action. There is no market for PISP access to payers' accounts with each bank, as each bank is the monopolistic provider of access to their own customers' accounts, therefore, no market driven price can be achieved. VRP non-sweeping must follow the precedent of single open banking payments, Faster Payments and Direct Debits, whereby the service provider enabling the innovative payment method (the PISP in VRP) is not charged, but instead the party receiving the service: the business collecting payment. This model ensures there are two competitive markets holding suppliers to account and delivering revenue streams: a competitive market for business bank account services holding the banks to account, and one for service providers (PISPs) holding PISPs to account. Any other charging model, aside from constant and continual regulator price monitoring and capping, is unworkable; even taking a regulator price monitoring and capping model, the price would have to be capped at such a level as to still incentivise a business to integrate a new payment method in a challenging economic climate.

Managed roll out across sectors

Much has been raised about 'liability' which, in our view, is covered by the Payment Services Regulations 2017 and/or via the Contingent Reimbursement Model for APP scams or other existing legislation such as the Consumer Rights Act 2015. We detail our further thinking regarding APP scam fraud in the sections below. With this accommodated, the benefits of VRP beyond sweeping for businesses and consumers are numerous, and are helpful in a struggling economy, and a cost of living and energy crisis; it is not therefore an appropriate balance of risk and benefit to delay extending VRP beyond sweeping, particularly into the energy sector, for unexplained and unsubstantiated claims of liability ambiguity.

We propose that beyond sweeping VRP be mandated on the CMA9 (and ideally all ASPSPs) for regulated sectors, where consumers are already protected by overseeing regulators and where business behaviour and action is already monitored and measured. This would encompass and afford roll out of beyond sweeping VRP immediately and safely to:

- Utilities, energy and water,
- Telecoms,
- Financial Services,
- Professionals services such as legal, accounting, medical,
- Housing,
- Education, and
- Charities.

We detailed our arguments further in a previous letter to JROC, as set out in Annex 2 to this response.

Require alignment between ASPSP live and sandbox environments

Currently there is a gap between an ASPSP's live environment and sandboxes, meaning that not all use cases can be tested in a scalable and sustainable way. To test capabilities, TPPs have to open personal accounts or use crowdsourced testing suppliers, which limits the ability to run testing at scale and precludes the TPP's ability to test business and corporate accounts. As part of the baseline, ASPSPs should close the gap by either aligning sandbox and live environments or enabling TPPs to test live.

ii. Evolving the broader regulatory framework to support open banking

Relevant consultation questions:

1. How should the payment services framework evolve – and what should be the government's priorities – to better promote the following government objectives for payments regulation:
   A. Achieving agile and proportionate regulation, which facilitates the international competitiveness of the UK economy through growth and innovation in the UK payments sector
   B. Ensuring appropriate trust and protection for consumers
   C. Ensuring the resilience and integrity of the UK's payment market
   D. Fostering competition, in the interests of consumers

24. Finally, do you have any other observations relating to the payments framework not encompassed above, and how this could be further improved, in line with the government's objectives?

Empower the Future Entity

There is uncertainty about how the successor to OBIE will derive its powers, what powers it will have, and its abilities to enforce those powers. This is stalling the development of open banking payments to a near crippling extent, and urgent clarification is necessary.

It is fundamental the open banking ecosystem, if it is to compete with banks and cards, that the Future Entity can direct participants to implement standards and is empowered to oversee API implementation and monitor and enforce adherence to standards by ASPSPs and TPPs. Poor API service levels, repeated unplanned downtime and other obstacles should trigger automatic sanctions on ASPSPs.

iii. Emerging fraud threats and open banking

Relevant consultation questions:

19. Are consumers adequately protected from evolving fraud threats under the existing legislation – is further policy needed to ensure this, and how should that policy be framed?

20. In relation to payment transactions which payment service providers suspect could be the result of fraud, is there a case for amending the execution times for payments to enable enhanced customer engagement? What requirements should apply here to ensure the risk to legitimate payments is minimised and that such delays only apply to high-risk, complex-to-resolve cases?

21. In relation to fraud, whether unauthorised or authorised, is there a need to a) complement rules with data sharing requirements; and b) for further reforms be made to make Strong Customer Authentication work more effectively and proportionately?

Whilst not ignoring that *some* payments are fraudulent and that there must be efforts by all parties to prevent fraud from happening and enforce fraudulent penalties once fraud has occurred, the reality is that the vast majority of open banking payments are legitimate. Therefore, in line with regulatory and government objectives, to preserve and support the growing but still nascent open banking market, it is imperative that open banking is seen to be consistent, reliable and operational.

Open banking being and being seen to be consistent, reliable and operational is not supported when banks stop open banking payments due to either being a first payment to a new payee, and/or if the amount is ≥£1,500, on the grounds of unevidenced suspicion of fraud; and further, when a payer acts on a bank message to call their bank to check the payment they are trying to make, are told that they should not use PISPs to make payments as they are unsafe and they should use their own bank's channels or a card, as some of our end users have experienced.

The result of this bank behaviour is that business merchants and their customers get the signal that open banking is not for every day reliable use and they stop using open banking, to the detriment of TPPs, the open banking market and the UK's success. What is imperative is to enable the open banking market to operate (which paves the way for open finance and open data), is for *payments* to *flow*, and fraud to be stopped.

The current regulatory framework causes bank behaviour that may stop some fraudulent Faster Payments, but which definitely makes all legitimate Faster Payments more difficult to use by payers.

Instead, to keep payments flowing, which is what supports an innovative consumer benefiting market, fraud prevention needs to focus on preventing paid funds being credited to criminally operated bank accounts, rather than stopping many payments being sent at all, a small proportion of which *might* be fraudulent. This change will benefit all Faster Payments (including open banking) by avoiding false positives interrupting the sending of payments and focussing prevention onto receiving banks properly KYCing their customers and overseeing the operation of their accounts – an existing AML requirement anyway. Receiving banks, unlike sending banks, should know who their payee customers are, are in a much better position to spot unusual usage of their accounts, and can trap repeating low value frauds, not just higher values. When a receiving bank is suspicious of a receipt it can prevent those funds being credited to their customer prior to investigation. In this model false positives have almost zero impact on the conduct of normal commerce. Once a bank understands the operating model of a legitimate, but previously suspicious, customer, further false positives can be avoided for subsequent payments to that customer.

This model, allows a payment to flow from a sender's account, and it being delayed and ring-fenced once at the receiving bank if fraud is suspected. This gives the better placed receiving bank time to conduct checks to establish fraud or otherwise, is also a more effective solution than simply delaying payments to D+1 and hoping the sender realises they have been scammed in time.

To the extent that more time should be allowed for ASPSPs to investigate suspicious payments, for the reasons outlined above, this must be restricted to receiving banks being allowed to delay credit to a payee's account pending payee investigation – this is likely to be most effective and least disruptive to legitimate commerce whilst catching fraud. It should not apply to the sending bank unless the ASPSP has legitimate concerns only about account take over, and even these concerns should be resolvable within the current time limits. If an ASPSP has concern about its customer's credentials for authorising a payment via SCA it should probably block all access via SCA and contact the customer to resolve its concerns.

A corollary of this approach is that reimbursement for scams (or as we see it, hosting a bank account for a criminal, or for criminal purposes) should apply 100% to the payee's bank. The payee's bank is enabling the criminal activity, has the best intelligence to stop this, and already has AML and KYC obligations. Sending (payer) banks can add very limited value to stopping fraud and are much more likely to contribute to false positives and the interruption of legitimate commerce if they are responsible for any part of reimbursement, beyond their own failure to undertake SCA on their customer's payment authorisation properly.

The priorities and mandates outlined above are crucial to the growth of the open banking market in the UK, and are essential considerations for the review of the PSRs. Without such action, the success of FinTech and open banking in the UK is severely threatened.

Annex: Previous letter to JROC

JROC Open Banking Breakthrough Opportunity 220223

Through a minimal regulatory intervention, JROC can quickly open up many VRP non-sweeping payments to provide their benefits to businesses and their end-customers without risk and inappropriate negative consequences for consumers and their ASPSPs.

- Consumer and ASPSP risk can be fully mitigated by restricting merchants to agreed regulated sectors.
- A critical mass of VRP supporting ASPSPs (CMA9) must be mandated to permit their current sweeping service to be used by this broader category of merchants. There are no incremental development costs to ASPSPs to support this. Without a regulator mandate ASPSPs will continue to act anti-competitively to protect their card revenues by not offering the service.
- The existing charging model for single payments and sweeping VRP must be extended to this new merchant category because there can be no commercial market in VRPs due to the de facto monopoly provision of individual ASPSPs. ASPSPs will be appropriately compensated through their existing competitive Faster Payment charging.

As there are no ASPSP technical developments or intra-business processes needed to support this expansion (the FCA can provide oversight of TPP regulated merchant on-boarding), and TPPs like Ordo have these broader VRP services ready to go, the considerable benefits of this important open banking extension can be delivered immediately.

Rationale and Supporting Evidence

At the end of January, we wrote to JROC participants and HMT to outline the small number of critical actions we think JROC should take to enable open banking to deliver to its potential for consumers and businesses in the months and years ahead. These actions included enabling PISPs to offer VRP enabled services beyond sweeping. The recently published final report of the Strategic Working Group (SWG) has revealed an opportunity to do this in a way that we think addresses the legitimate concerns of ASPSPs and consumer champions, delivers much broader application and benefits from VRPs now, and importantly requires no further technical developments by ASPSPs or TPPs.

A central recommendation of the SWG is to extend open banking by providing VRPs for non-sweeping use cases (Final report section 1.1.5). SWG reports that there is significant stakeholder appetite to deliver additional payments functionality with VRP in more use cases (1.4.1) and that a

short-term priority should be to evaluate the use of VRPs in low-risk sectors as this will "*provide an opportunity to maintain the momentum of this new open banking capability*".

SWG seems to identify three broad questions that need to be addressed to allow this to happen:

1. The risk to consumers and their banks from errors and abuse needs to be managed.
2. A critical mass of supporting banks needs to be reached either through voluntary actions by banks or regulatory pressure/action.
3. An effective and fair pricing model needs to be agreed/mandated between users, ASPSPs and TPPs.

Synthesising the relevant contents of the final SWG report these three questions can be addressed in the following ways.

Managing risk to consumers and their banks

The central concern raised by external experts on behalf of consumers and ASPSPs is that extending VRP beyond sweeping will leave consumers without any protection or recourse if a merchant abuses VRP and that ASPSPs might suffer liability if, for example, extended VRPs were used to support Authorised Push Payment (APP) scams. The SWG report gets close to a simple solution when it suggests expansion to lower-risk sectors like government, Utilities and regulated investments (1.14.2.3).

A clear and straightforward way to ensure that appropriate consumer protection is provided would be to expand VRP use cases to merchants operating in regulated sectors that already provide comprehensive and legal consumer protection from abuse by suppliers, and redress and complaint routes such as ombudsmen. As a start this could cover all merchant businesses/organisations regulated by the FCA, the PRA, Ofgem, Ofwat, Ofcom, The Charities Commission and central and local government departments and agencies. This provides clear merchant acceptance criteria (for TPPs to manage) and ensures that consumers will have full redress for errors or abuse when dealing with these organisations. This should fully mitigate the consumer and liability risks reported into the SWG process. The issue is not the particular use-case, it is the trustworthiness of the merchant and available consumer protections that drives this. This approach also provides precision on which merchant is allowed compared to the complex and subtle rules that try to define the boundaries of sweeping.

Restricting access to regulated merchants in this way would eliminate APP scam risks via VRP as APP scams require the receiving bank account to be controlled by the criminal.

Achieving a Critical Mass of Supporting ASPSPs

The SWG report is clear that voluntary expansion by enough ASPSPs into VRPs beyond sweeping is unlikely. Extending VRPs to non-sweeping was championed by TPPs, but not many ASPSPS (1.14.1.2). There was also wide agreement that commercial realities are unlikely to lead to the expansion of VRPs, especially in the short term (1.14.2.3).

It is evidenced through our own interaction with ASPSPs that a critical mass of ASPSPs (say the CMA9) is not going to voluntarily support use cases beyond sweeping because enabling this new competition is not in their commercial interests – some are overt about this, others simply decline to go beyond sweeping. Non-sweeping VRPs will shift payments from ASPSP's credit and debit cards, reducing their interchange fee revenues and, if these new services are to be competitive for merchants, are not likely to be offset by any charges they raise for VRPs or the underlying Faster Payments.

In the same way that sweeping VRPs would not have been supported unless mandated by the CMA as a competition remedy, expansion to new merchant types will not be supported by ASPSPs

unless mandated by the FCA/PSR as an action to prevent the larger ASPSPs blocking this new competition.

It is important to note that, given the work they have done to support sweeping, impacted ASPSPs will have to undertake no additional development to support these broader merchant categories, so the only 'cost' to the ASPSPs will be lost card revenue through new competition.

Finding an Effective and Fair Pricing Model

The SWG report lays out four different options for pricing of VRPs, briefly:

- Access should be *free** (our italics, see below) in line with other Payment Initiation Services.
- Commercial agreements should be market driven.
- Price, or a price cap should be set by an appropriate regulator.
- Commercial fee arrangements should be set centrally by an independent body.

There are a number of factors that should influence the choice of pricing option that don't seem to have been adequately covered in the SWG report, but once considered quickly lead to a single approach for VRP commercials. Specifically,

- Throughout the report the current provision of Payment Initiation Services, including VRP sweeping, is characterised as "free", strongly implying that ASPSPs are not compensated for executing these open banking payments. This is wrong. Open banking allows, and indeed requires, ASPSPs to charge their customers for open banking Faster Payments as they do for their own Faster Payments. They typically charge businesses for sending and receiving Faster Payments, either individually or as part of an account monthly fee. For consumers, competition between banks means that the costs of all payments (including Faster Payments, Direct Debits, Bacs receipts and Cheques) are recovered via monthly fees or forgone account balance interest. If this model were extended to all VRPs, then ASPSPs would continue to receive compensation for executing these payments from the underlying Faster Payments charges.
- There can be no market mechanism for setting a commercial price for executing a VRP. In order to deliver a VRP enabled service a TPP must have VRP coverage for each bank that each end-customer might wish to pay from. For a Barclays end-customer/payer a TPP must buy VRP from Barclays, other ASPSPs are not a substitute. An ASPSP has a de facto monopoly on the provision of VRP for its own paying customers (this is analogous to telecoms provision of call termination, which has to be price regulated as a consequence). As there are no competitive constraints, ASPSPs that are offering VRP beyond sweeping are setting their price at a high enough level, and as a percentage of payments value, to ensure that they are fully offsetting any losses of revenue from card interchange fees they may suffer.

Given that there is no market mechanism available to establish fair pricing for VRPs then a central, probably regulated, price could be established, perhaps using a Long Run Incremental Cost (LRIC) basis. However, this is administratively unattractive and unnecessary as simple application of the current single payment and VRP sweeping pricing model (where the payment is paid for by the merchant and sometimes the end-customer) works and is incidentally the model used for Direct Debit charging for many years. It provides fair recompense to ASPSPs and maintains competitive pressures. If a merchant is unhappy with the Faster Payment charges it receives from its ASPSP to receive VRPs, it can shop around for all or part of its banking services. The same would apply for consumers if the current free-in-credit charging model for payments changes in the future.