# The Future Development of Open Banking in the UK

Final report for the Joint Regulatory Oversight Committee

February 2023

Open Banking Strategic Working Group Secretariat

# FOREWORD

In March 2022, HM Treasury, the Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA) and the Payment Systems Regulator (PSR) announced the creation of a new Joint Regulatory Oversight Committee (the Committee) as part of the Government and regulators' commitment to build on the success of open banking. The Committee is determined to ensure that the benefits of open banking are fully realised, and momentum is sustained. The industry and other key stakeholders, including consumer and business representatives, play an instrumental role in delivering these outcomes and the Committee has been keen to work closely with the ecosystem to shape the future development of open banking.

To support this, the Committee convened the Strategic Working Group (SWG), a non-decision-making consultative forum independently chaired by Bryan Zhang, to enable industry and stakeholders to share their views and input into the vision for the future of open banking.

This final report provides extensive analysis and will form an important part of the input for the Committee to consider as it develops its recommendations. The Committee aims to publicly set out its recommendations relating to the vision for open banking, alongside the design of the Future Entity, in Q1 2023. We expect it to include a roadmap to deliver that vision. Ahead of that publication, we are keen to continue engaging with industry and broader stakeholders. Open banking can only deliver its full potential if authorities and broader stakeholders work together.

Finally, we would like to thank Bryan Zhang and the SWG secretariat for overseeing a process that has enabled wide-reaching stakeholder engagement and delivered a broad base of evidence and insight at pace. We would also like to thank all the participants.

**Sheldon Mills**
**Co-chair,**
**Joint Regulatory Oversight Committee**

**Chris Hemsley**
**Co-chair,**
**Joint Regulatory Oversight Committee**

# PREFACE

UK open banking is at a crossroads. Under the CMA Order the open banking ecosystem developed rapidly and has brought benefits to millions of consumers and businesses. Looking beyond the horizon, questions remain about its future direction, scalability and sustainability. The SWG process was initiated by the Committee to examine these questions by consulting with a wide range of ecosystem stakeholders, collecting empirical evidence at scale and collating views at pace, to inform the development of a future roadmap for open banking in the UK.

Between September and November 2022, the SWG Secretariat designed and executed a series of strategy sprints under the guidance of the Committee to understand better how to unlock the potential of open banking payments, develop further data sharing propositions and ensure a sustainable open banking ecosystem. The SWG process achieved a high level of engagement thanks to the support and contribution of industry associations, fintechs and account providers, end user representatives, independent subject matter experts, and other key ecosystem stakeholders, resulting in 189 written submissions from 104 organisations.

It was my great pleasure and privilege to independently chair the SWG process and work with stakeholders and experts across the UK open banking ecosystem. I was constantly in awe of people's passion for open banking and their drive to propel financial innovation to better serve consumers and SMEs, whilst robustly protecting their safety and interests. It was also apparent that many key issues are complex and fluid; firms and institutions can harbour highly nuanced perspectives and it would be wrong to assume homogeneity in any stakeholder group or even within an organisation; and while the evidence did highlight the existence of divergent views, common ground and areas of alignment were also to be found. In essence, the challenges and opportunities facing the UK open banking ecosystem are not unique, but intrinsically part of the financial innovation process, which requires sound evidence, common understanding, multi-stakeholder collaboration, strategic thinking and collective will for it to sustain, scale and benefit end-users and the wider economy. I hope this report will go some way to help establish that evidence-base, develop a common understanding, facilitate collaboration, crystallise strategy and inform the decision-making by the Committee.

The structure of the report mirrors the framework we adopted for the two rounds of open banking strategy sprints. The first half of the report focuses on gap analysis, which aims to understand key gaps between the current state of open banking and a more optimal future state. It also analyses how various stakeholders perceived these gaps and examines possible drivers underpinning their perceptions. The second half of the report focuses on exploring a diverse range of potential solutions, both in the short-term and in the long-term, that could bridge those gaps, 'level up' the ecosystem and make it 'fit-for-purpose', including a discussion on the future industry structure based on the evidence collected and views collated.

The SWG process wasn't without its flaws and this report is by no means conclusive. I would like to take this opportunity to express my gratitude to all participants of the strategy sprints for their invaluable contribution to the process, despite the very challenging timeline. I am also immensely indebted to the SWG Secretariat for its hard work, dedication and exemplary professionalism. Finally, I would like to thank the Committee for its support and guidance. As the UK embarks on a new chapter of open banking development and looks into the future of open finance and smart data, I trust that the entire ecosystem will rise to the challenge and seize the opportunity.

**Bryan Zhang**
**Independent Chair of the Open Banking Strategic Working Group**

# ACKNOWLEDGEMENTS

This report, and the open banking SWG process it draws the evidence from, would not have been possible without the support and dedication of numerous individuals, institutions and stakeholder groups across the United Kingdom open banking ecosystem.

We would like to thank the Joint Regulatory Oversight Committee and in particular the co-Chairs Sheldon Mills and Chris Hemsley, for giving us their trust, time and support. We would also like to thank colleagues at the Financial Conduct Authority, the Payment Systems Regulator, the Competition and Markets Authority and HM Treasury, especially Helene Oger-Zaher, Alice Mackay, Teresa Lam, Jeroen de Marteau, Ciaran Gill, Marc Maxfield and Andrew Self, for their guidance and expertise.

The SWG process and the series of Strategy Sprints could not have been completed without the support of the following industry associations including: the Electronic Money Association, the European TPP Association, FDATA Global, Innovate Finance, the Open Finance Association, The Payments Association and UK Finance. These key open banking ecosystem stakeholders kindly devoted considerable time and effort to participate in the SWG meetings and nominated contributors for the Payments Strategy Sprints and the Data Strategy Sprints.

We would also like to thank all participants of the Open Banking Strategy Sprints, both for the evidence submitted and their input into the discussion sessions. It is also important to acknowledge and thank the large number of respondents who were not members of the SWG and expert panels but who also contributed valuable evidence and insight that informed the discussion sessions and the final report.

Finally, we would like to thank Charlotte Crosswell, Chair and Trustee, and Henk Van Hulle, CEO, at the OBIE for providing resources to enable the independent functioning and working of the SWG Secretariat. We would like to thank several OBIE colleagues that provided administrative, communication and design support, in particular, Adrienne, Fiona, Matt, Patrick and Sam.

**The SWG Secretariat**

# SWG SECRETARIAT

The SWG Secretariat consisted of the following individuals who designed and facilitated the series of Open Banking Strategy Sprints and co-authored the final report based on the evidence gathered and views collated during the SWG process:

- **Bryan Zhang – Independent Chair of the SWG**
- **Alan Ainsworth – Member of SWG Secretariat**
- **Richard Mould – Member of SWG Secretariat**
- **Richard Koch – Member of SWG Secretariat**
- **Daniel Jenkinson – Member of SWG Secretariat**
- **Deborah Horton – Member of SWG Secretariat**
- **Shannon Kingston – Member of SWG Secretariat**
- **Simon Marsh – Member of SWG Secretariat**
- **Matthew Wallace – Member of SWG Secretariat**

# EXECUTIVE SUMMARY

More than 6.5 million consumers and SMEs in the UK already use open banking-enabled products and services, contributing to UK leadership in the fintech sector, with UK citizens and businesses benefiting from increased competition, choice and innovation.

Last year HMRC stated that their adoption of open banking had saved the public purse over £500k in bank fees[1] with more than £10.5bn tax collected to date through open banking payments, demonstrating the efficiencies this new capability can deliver. In January 2023 the CMA announced that the six largest banking providers had implemented all the requirements of the Open Banking Roadmap[2]. In order to build on this success, the Government and regulators set up the Joint Regulatory Oversight Committee ("the Committee") to take forward the development of open banking beyond the CMA Order.

The co-chairs of the Committee, the FCA and the PSR, convened a Strategic Working Group (SWG) to collect empirical evidence and collate views from industry and other stakeholders to input to the future development of open banking in the United Kingdom.

The SWG created an open banking strategic sprint process to address questions set by the Committee under three priority areas:

**Payments Strategy Sprint:** Unlocking the potential of open banking payments
**Data Strategy Sprint:** Promoting further data sharing in an open banking framework
**Ecosystem Strategy Sprint:** Ensuring a sustainable open banking ecosystem.

The process elicited a broad base of evidence and opinions about the future of open banking and ways to best deliver that future. In total, over the course of two rounds of strategy sprints conducted from September to November 2022, the SWG Secretariat received **189** written submissions from open banking industry stakeholders, end-user representatives and independent subject matter experts.

The first round of strategy sprints identified five main gaps between the current state and what many respondents suggested was a more optimal future state for the UK open banking ecosystem. The second round of sprints focused on identifying a range of possible solutions, both short-term and long-term, that could bridge these gaps to unlock the potential of open banking payments, further data sharing propositions and build a more sustainable open banking ecosystem.

It was evident throughout the SWG process that key stakeholders of the open banking ecosystem share a desire for open banking to work well for consumers and businesses, enabling them to take advantage of new ways to manage their finances and have more options for payments in a safe environment.

However, despite this common desire it is evident that stakeholders have considerably different views when it comes to the detail of how to achieve this. It is also clear that many stakeholders have differing visions for the future of open banking and varied views on the forward-looking agenda, including on the structure and funding of a Future Entity (or entities). This report aims to reflect divergent views on key issues and identify areas of potential or emerging alignment. It

[1] https://www.globalgovernmentfintech.com/hmrc-open-banking-rollout-takes-in-24-more-tax-types/
[2] https://www.gov.uk/government/news/millions-of-customers-benefit-as-open-banking-reaches-milestone

provides empirical evidence to assist the Committee in considering and making decisions that will shape the future of open banking in the UK.

## 1.1. Gaps and Perception of Gaps

The first round of strategy sprints focused on gap analysis and examined empirical evidence collated from open banking payments, data and ecosystem sprints. The evidence received suggested that there may be a number of gaps between the current and a more optimal future state of open banking ecosystem. It is worth noting that since there is limited consensus on what the future state entails, these gaps and the *perception of them* are often contested, with stakeholders harbouring different views on their relevance or extent.

### 1.1.1. Ecosystem Reliability

The evidence pointed to a possible API availability and performance gap. Whilst some respondents felt that firms' APIs had been performing well, improved over time and were meeting their obligations, others were frustrated by the inconsistency of API provisioning and argued that further improvement was required to provide a more stable and reliable platform for open banking. Further evidence illustrated a significant variance in conversion rates across firms, and across channels (mobile app vs. desktop). Expert advisers also highlighted the growing criticality of open banking reliability, particularly in the small business market where down-time or non-availability have a particularly damaging impact.

Whilst all distributed networks will inevitably exhibit variance, the magnitude of variance in performance and consistency was such that it was reported by some to undermine the reliability of the whole system. Such participants felt that this was another clear indicator that improvement was needed across the ecosystem and that there was an opportunity to "level up" to the performance of the best.

In addition, the availability and quality of the performance data was limited and did not cover the whole of the market. Whilst the CMA9 firms submit performance data, this is only a subset of the market. Some TPPs provided data on availability and conversion rates but this had also not been subjected to independent scrutiny.

### 1.1.2. Fraud

There was alignment across all stakeholders on the importance of ensuring that consumers and SMEs are appropriately protected from fraud, in particular APP scams, when using open banking payments. However, there were differing views on the appropriate response to this challenge. ASPSPs and TPPs often had divergent views as to the quantum of new fraud risk introduced (or reduced) by open banking payments. The evidence surfaced during the strategy sprint to support the different positions, although useful, can be anecdotal, not sufficiently representative of the whole market, or at too high a level to determine with confidence the extent, severity and root causes of fraud.

Many TPPs believe that banks' current counter-APP fraud measures can have a significantly detrimental effect on customer experience which undermines the reliability and viability of many open banking use cases. They argued there were many cases of 'false positives' and provided evidence that some ASPSPs' counter-fraud measures could add excessive 'friction' in customer journeys, and could restrict the development of the open banking payments market. High-value payments are particularly impacted by fraud prevention measures, resulting in lower conversion rates and customers of some ASPSPs being excluded from certain use cases.

However, some ASPSPs highlight that attempted and successful fraud in open banking channels is higher than other channels, in some cases twice as high, based on their internal data. Therefore, they believe that counter-fraud measures currently in place are necessary and proportionate.

There was widespread agreement that a robust evidence base was required to better assess fraud and fraud prevention methods in open banking payments. A number of respondents also highlighted the importance of considering the impact of the PSR's potential changes to the way in which APP fraud liability was allocated, which could have far-reaching implications for the way in which open banking payment fraud is managed.

### 1.1.3. Enhancements to the existing standards

TPPs, some ASPSPs and expert advisers highlighted several gaps in the UK Open Banking Standard which prevent open banking from better meeting end user needs. In contrast, most ASPSPs typically felt that there was a limited case for any mandated enhancements of the standard. Some of the improvements highlighted include:

- Requiring the use of more granular and consistent error codes and messages, to help TPPs understand if something isn't working and to communicate more clearly with end users.
- Enhanced payment functionality (e.g., payment status or payment certainty), to enable TPPs to have greater clarity as to whether a payment initiation has resulted in a successful payment and so better meet the needs for retail payments.
- Enabling identification of participants in the payments and data flow to be shared in the consent journey, rather than by software statements, and thereby bring greater clarity and visibility to end users on the end recipient of data or beneficiary of payment.

### 1.1.4. Customer protection and trust

All participants recognised the need to ensure that customers were protected and able to obtain redress if something went wrong. However, how this should occur and who should carry liability for it were topics of significant divergence.

The need and design of a customer protection regime for account-to-account payments demonstrated a very broad range of often contradictory positions across the ecosystem, particularly in terms of the scope and coverage of protections that should be provided:

- Many ASPSPs and expert advisers argued for broad protections. These responses highlighted the differential between the customer protections offered by card payments via Section 75

and chargebacks and those available in open banking payments. Closing this differential was required to support the expansion of open banking into other markets in their view.

- Some concerns were raised that the cost of provision of similar protections would increase the cost of open banking payments comparatively, reducing the motivation to shift payments.
- One expert adviser highlighted that the chargeback rights of cards was complex and what was needed was a reliable and trusted method of payment.
- Several TPPs questioned the extent of a gap in this space, highlighting the clarity of the Payment Services Regulations in terms of payment disputes (e.g., unauthorised transactions, payment errors). Purchase protection (e.g., goods or services not received, bankruptcy) in their view was a matter between the consumer and the merchant, with many situations covered by existing protections if a consumer and merchant are unable to resolve an issue.

Some submissions suggested that education and communication may be one way to resolve the impasse, but others challenged the view that consumers, particularly those in vulnerable circumstances, would be able to discriminate between payment types and understand the implications of the different protections offered.

As is to be expected, the issue of liability for the different types of consumer protection, (e.g., purchase protection, fraudulent merchants, payment errors etc.) also brought out divergent views from stakeholders.

Trust was also a topic which prompted divergent views, with some large ASPSPs suggesting that the current growth of the ecosystem indicating that trust was not a barrier. Others called for a range of interventions to enhance trust, including communication, improvements in clarity of language, education or trust marks.

### 1.1.5. Extension of open banking

Providing access to Variable Recurring Payments (VRPs) for non-sweeping use cases was referenced in many of the submissions and there was divergence in how this service should be brought about and the cost for access. Some TPPs recommended that access to VRPs for non-sweeping use cases should be mandated on all the banks for all use cases. In contrast, ASPSPs recommended that the offering of VRPs should be voluntary and be market-driven. Expert advisers and some ASPSPs recommended ensuring that a liability framework and customer protection regime (including redress mechanisms) is in place before extending VRPs beyond sweeping. A range of possible options for the pricing of VRPs, which cut across respondent communities, emerged as:

- **Access to VRPs should be free in line with other payment initiation services; or**
- **Commercial agreements should be market-driven; or**
- **Price, or a price cap, should be set by an appropriate regulator; or**
- **Commercial fee arrangements should be set centrally by an independent body.**

The expansion of data sharing beyond PSD2 was an area with widespread support. Most TPPs and all expert advisers were of the view that an evolution to open finance was essential as soon as possible. However, there was t also divergence of opinion across the ecosystem regarding which data sets should be shared, what the priorities were and the drivers for expansion. Some participants cited customers not understanding why certain savings products can be seen in open

banking powered services but not others. Some respondents felt that sharing data on lending products and other financial products would be of value to customers, particularly those in vulnerable circumstances and to small businesses. It was noted that access to a wider pool of data could provide new tools and resources to help consumers navigate the cost-of-living crisis.

The sharing of identity attributes was regarded by some as an important development of the market, particularly to widen access and address exclusion, whereas others felt that what was most important was that any initiatives aligned to the UK digital identity and attributes framework, and existing identity initiatives (such as The Savings and Investment Alliance (TISA)) and to not duplicate efforts.

The need for the wholesale expansion of open banking payments to support e-commerce is another area where there is a perception gap in the long-term vision for open banking. Some respondents felt that this development was important to provide a viable alternative for card payments, whereas others felt that the issues of customer protection and a viable commercial model need to be addressed before expansion of open banking payments is progressed.

## 1.2. Plausible Drivers for Divergent Views on Gaps and Perception of Gaps

There is a myriad of plausible explanations why these gaps or perceived gaps exist among open banking ecosystem stakeholders. From the written submissions and sprint discussion sessions, it is evident that two of those plausible drivers for divergent views are: a) the lack of key empirical data and b) difference in visions for open banking.

### Lack of key empirical data and resulting inconsistency in interpretation

In order to have an evidence-based approach to resolve some outstanding issues within the open banking ecosystem and discuss future development, various stakeholder groups need to have access to up-to-date, consistent data sets to shed light on key issues such as API reliability and fraud.

In terms of API reliability, there are simply no ecosystem-wide data sets of the performance of the entire open banking ecosystem, nor is the available MI broadly available. The large ASPSPs report on API performance, but the response from the TPP community was that this does not reflect the effective performance of the system and so additional metrics may be required. For example, the evidence submitted by TPPs often cited customer journey completion rates as a more appropriate metric than API performance. Other firms in the ecosystem are not subject to the same mandated requirement of reliability or reporting under the current regime.

Given the strongly opposing views regarding tackling APP fraud, a more detailed and broad evidence base would help ensure that there is a common understanding of where the actual and potential vulnerabilities in open banking payments lie. This would enable ecosystem stakeholders to determine the prevalence, extent and severity of fraudulent activities within the open banking ecosystem and how it compares to other channels. This is very important for stakeholders to have the same point of departure and work collectively on risk-based measures and fraud-related issues.

There was also a lack of evidence of the cost to implement many of the developments. Large ASPSPs often cited the lack of a business case for further developments whilst TPPs tend to advocate for them. More data and evidence both on the cost side and the opportunity side (perhaps through consumer and SME end-user research or/and looking at examples from other jurisdictions) would enable evidence-based cost-benefit analysis.

### Different perspectives on the future

From the responses received, stakeholders agreed with the broad direction of the vision, but had different levels of ambition and varying views on how to achieve it. For most ASPSPs that participated in the strategy sprints, further evolution of the open banking ecosystem needs to be underpinned by reasonable commercial returns and the market should determine the development path. Some trade associations and TPPs echoed this market-centric vision of the future. However, many TPPs expressed concerns about relying solely on market forces to steer the development of the open banking ecosystem. Expert advisers also echoed the need for regulatory direction, highlighting previous examples of initiatives which had made little progress without clear regulatory mandate.

### Lack of aligned incentives

A misalignment of incentives underpins many of the gaps discussed above. For instance, in terms of ecosystem performance, ASPSPs often cited the regulatory obligation to provide parity of

performance with their digital channels and claimed that this was met. There is often limited incentive for ASPSPs to invest further funds to deliver more than the regulatory minimum. Some TPPs would question the extent to which parity has been achieved and many more wanted further improvements in performance to support wider adoption of open banking.

The situation is similar regarding fraud, whilst respondents from across the ecosystem expressed a strong desire to reduce the levels of fraud as well as the number of false positives (where a legitimate transaction is blocked), the incentives may differ across various stakeholder groups. For a bank, a false positive causes inconvenience for their customer, but the customer typically has an alternative way to pay, and the consequences of not stopping a fraudulent transaction would have a greater adverse impact on the customer and the bank (as they may have to refund the customer). For a TPP offering payment services, a blocked transaction results in not being able to provide a service to their customer and so undermines their whole business. Consequently, this may impact the ability for banks to invest in capabilities to deliver the level of granular risk analysis that TPPs desire (e.g., some uses cases, such as paying taxes, are less susceptible to APP fraud, but are believed to be treated in the same way as other open banking transactions and so have the same transaction limits).

Furthermore, at present there are limited commercial incentives to support the wholesale extension of open banking. From the evidence, it is a challenge to see the emergence of a scalable commercial model to support the voluntary expansion of VRPs for non-sweeping use cases and overcome the potential barriers of customer protection and liability. At present there is also no or limited incentive for data holders, such as savings or loan providers, to open access to further data sets to support open banking access to savings or loans. Provision of access would require investment and clarity on regulatory permissions or contractual frameworks, and without a suitable pricing structure there is limited commercial benefit to the data provider.

There are also mis-aligned incentives around the expansion of open banking payments to support ecommerce. Provision of open banking payments as a viable ecommerce payment option represents a market expansion opportunity for TPPs, but for ASPSPs it would potentially cannibalise existing interchange revenue streams and add costs if there is a need to handle more payment disputes. Given the downside risk for ASPSPs, there is a limited investment case to improve open banking system performance and functionality beyond the regulatory requirements.

Despite these at times misaligned incentives, there was significant common ground on the aspiration to develop open banking for the benefit of the UK’s people and small businesses.

## 1.3. Potential Short-term and Long-term Solutions to Bridge Gaps

The second round of strategy sprints focused on discussing a wide range of solutions, both in the short-term and long-term, that could potentially bridge ecosystem gaps, unlock the potential of open banking payments, further data-sharing propositions and put the development of open banking on a more sustainable footing. As in the first round of strategy sprints, there is still limited consensus on what solutions should be prioritised, how actions could be sequenced or the mechanism(s) (e.g., regulatory or market-driven) through which a workable agenda can be delivered. ASPSPs stressed the importance of carefully considering the costs and benefits, and assessing need/demand, of any expansion of Open Banking, prior to embarking on developing solutions. There are also widely divergent views on the structure and funding of Future Entity or entities, underpinned by stakeholders' different visions and varying degree of ambition. Nevertheless, at least in the short to medium term, there seems to be some areas of alignment and potential workable solutions to move forward.

## 1.4. Unlock the Potential of Open Banking Payments

### 1.4.1. Thematic Priorities

Whilst there was a wide range of views on how to unlock the potential of open banking payments, the evidence identified three broad thematic priorities:

#### *Balancing fraud and friction*

This area addresses the question of how to effectively protect customers from fraud (in particular, APP fraud), without damaging customer experience through either declining legitimate payments or adding unnecessary friction. Excessive frictions during the customer journey may adversely affect payments completion rates, and the attractiveness of open banking payments, in particular high value payments, to both payers and payees.

#### *Improving ecosystem performance*

There is wide agreement that a stable and reliable platform is a required foundation block for open banking payments success. There is evidence that many propositions are not brought to market because ASPSPs, especially smaller providers, across the ecosystem do not provide consistently performing and available APIs, and because payment completion rates are inconsistent and/or low.

#### *Expansion of Variable Recurring Payments (VRPs) beyond sweeping*

There is significant appetite amongst stakeholder groups and particularly from representatives of the retail community, to deliver these additional payments functionality to more use-cases, despite the limited progress so far. However, it was recognised that VRPs have only recently been implemented, and only by the CMA9 for sweeping.

### 1.4.2. Possible Actions and Prioritisation

Whilst there is limited alignment regarding the actions needed to implement changes, there is a broad agreement that activities probably will need to be strategically sequenced and appropriately carried out to avoid any potential consumer detriment or unnecessary cost. There is also recognition that, whilst some actions may have external dependencies on, for example, revisions to the regulatory framework, it may be possible and desirable for some work to take place beforehand.

We have, as a result, set out such possible actions under three timescales – short-term (i.e., could start immediately and might have a short-term impact, time period 12 – 18 months), medium-term (i.e., could be dependent on the short-term activity, or more complex in nature to deliver, time period 18 – 36 months) and long-term (i.e., has external dependencies or implementation will be beyond 36 months). Some submissions highlighted the urgency of many of these actions and suggested that by working in parallel, even some of the longer term actions could start to be addressed immediately.

It should also be borne in mind that there is perhaps more clarity and alignment around what is required in the shorter term than in the longer term. Many of the activities suggested cut across more than one thematic priority.

## *Short-term priorities*

**Detailed evidence collection**

Stakeholder responses highlighted the need for better, and more granular, fraud data to be collected from across the ecosystem (i.e., from all ASPSPs as well as from TPPs), in order to help inform decision-making and the development of open banking payments. This is particularly needed to inform the debate about fraud and friction, where data is fragmented, inconsistent, and insufficiently detailed about use-cases and transaction values. In addition, whilst there is agreement that payment journey completion rates have improved over time, there is a significant disparity between some TPPs' evidence and that of ASPSPs.

**Transaction Risk Indicators (TRIs)**

There was a significant level of alignment that TRIs could be helpful in improving fraud risk assessment and therefore reduce the incidence of false positives, and that they needed to be implemented consistently across the whole ecosystem (i.e., all ASPSPs and TPPs). A phased approach to implementation was suggested by some respondents, starting with a technical implementation only. This approach could mitigate some of the concerns raised in evidence, recognising that 'fraud declines' and 'limit declines' are separate but linked items and may require different solutions.

**Standards enhancements**

There were strong calls from TPPs, independent stakeholders and CMA9 ASPSPs for the Open Banking Standard to be monitored and enforced across all ASPSPs in the ecosystem. There was also broad agreement especially amongst TPP communities that other short-term priorities include:

- **Improved status messaging,** i.e., informing the TPPs of the status of the payment, by providing the up-to-date payment status ASPSPs receive from the Faster Payments Scheme (FPS).
- **Improved error message consistency and granularity**, i.e., ensuring all ecosystem consistently apply current error codes, and adding additional codes to enhance the information flow from ASPSP to TPP, to help TPPs communicate with their customers.
- **Improvements to reliability across the whole ecosystem**, i.e., "levelling-up", which was suggested by both ASPSPs and TPPs, including a focus on downtime and dealing with the underlying causes of low payment completion rates.

**Evaluate the use of VRPs in low-risk sectors**

Many respondents and, in particular, representatives of retailers, expressed a strong appetite for the expansion of VRPs beyond sweeping, although several obstacles to this expansion such as the lack of a customer protection and disputes regime or the lack of a broad commercial arrangement were identified. However, the evidence also highlighted some potentially low-risk sectors for the expansion of VRPs, such as Government or utility payments. Evaluating ways to expand VRPs into lower risk sectors could provide an opportunity to maintain the momentum for this new open banking capability.

## *Medium-term priorities*

**Codes of Conduct and Multilateral Agreements (MLAs)**

The evidence provided suggested a range of mechanisms through which firms could work together to enable a wider range of payments solutions that are not currently available in the market. These mechanisms could be used to help solve multiple thematic priorities and could range from simpler solutions such as agreement templates, to more complex solutions which have features or components more akin to a payment scheme, such as trust mark, inter-firm compensation arrangements, customer redress process, and liability models. A number of submissions were sceptical that these issues could be effectively resolved without regulatory intervention.

There was little objection in principle to any of these proposed mechanisms, although many stakeholders provided evidence to suggest that the market did not require any of them at this time, and expressed confidence that ultimately, the market would find appropriate solutions if there were a need. Other respondents favoured more concerted efforts to bring firms together, with some (in particular TPPs and expert advisers) looking for regulatory intervention of varying degrees, ranging from providing regulatory cover for voluntary or commercial agreements to determining compensation arrangements.

The Secretariat, having considered the evidence provided, suggest that a phased approach may be appropriate, with each phase building on the previous phases' foundations and learnings, although many respondents highlighted that these phases would require some form of regulatory intervention in support. The phases of such an approach could be:

**Phase 1: Code(s) of conduct or rule books**

- Development of code(s) of conduct or rule books which all participating firms voluntarily agree upon. These would not be contractual but may enable trust to develop between firms (and potentially groups of firms) such that there is increased certainty as to the behaviour of a firm in a particular situation. For example, a group of TPPs could agree a methodology for implementing TRIs with a group of ASPSPs also agreeing to analyse their impact on APP fraud risk, with a commitment to jointly reviewing effectiveness and next steps. The Future Entity could play a key role in facilitating this.
- It is recognised that early phase activity could be supported by enabling a test environment (such as a regulatory sandbox), so that groups of firms could work together to better understand the potential customer impact and design appropriate levels of customer protection based on empirical data, and if necessary, make changes to the design of the code or rulebook, before making a commitment to implementation.
- Another example provided in evidence that could also be considered for a voluntary code or rule book is the extension of VRPs into a limited number of low-risk or lower-risk use-cases, with respondents suggesting these could include utility bills, charity payments, payments to Government, and moving money into regulated investments.

**Phase 2: MLAs**

- The development of MLAs was referenced several times as a potential solution for the extension of VRPs into multiple additional use-cases. Approximately two-thirds of respondents who mentioned VRPs believed that regulatory intervention would be necessary to expand VRPs beyond sweeping, and 43% favoured capped or zero pricing rather than leaving pricing to the market.
- Some responses also suggested that they could help address the other two thematic priorities, potentially as a progressive development building on earlier non-contractual codes or rule books. An MLA could cover issues such as liability, API performance and availability, customer protection and redress, inter-firm remuneration, and provision of additional technical functionality (such as "Premium APIs"). Many participants referenced the example of the EPC's SPAA scheme as an example of one way to encourage ASPSPs (or "data holders", as now referred to by the EPC) to provide additional payments functionalities (such as required to enable reverse payments or future-dated payments with no fixed amount).

### *Long-term priorities*

**Scalable VRPs scheme(s)**

Many expressed the view that the development of VRPs schemes could address a number of the identified challenges in the market. There was a wide range of views on the appetite for, nature of and desirability of regulatory intervention to facilitate the development of VRPs. Several respondents also suggested that VRPs could potentially resolve key open banking payments ecosystem performance issues, given the lower level of friction in VRP authentication compared to single immediate payments (SIPs).

**E-commerce scheme (or Account 2 Account Retail Transactions scheme – A2ART)**

Whilst there was very limited reference in the evidence to a potential A2ART scheme, many respondents wrote and spoke about the need for open banking payments to provide an alternative method for paying for goods and services, in particular online. Others, including some TPPs, saw open banking payments' extension and expansion into e-commerce and POS retail transactions being a relatively low priority area for now.

**Alignment with the NPA**

Whilst there is no clear demarcation between medium-term and long-term activities, many respondents felt that it was important for the development of open banking payments, particularly those requiring significant investment, to align closely with Pay.UK's New Payments Architecture (NPA). Examples cited included investing to deliver additional functionality such as payments certainty, and whether that would still be relevant in the NPA, due to its instant payment capability. Some ASPSPs suggested that Pay.UK and the Future Entity should work together to develop the long-term UK payments strategy, to reduce overlap and maximise the potential of both workstreams. Other respondents, largely TPPs, saw a more limited role for Pay.UK, and expressed concern that alignment to NPA could delay resolving some of the immediate areas of focus necessary to support the growth of open banking payments.

## 1.5. Promoting Further Data Sharing

### 1.5.1. Thematic Priorities

Whilst there were varying views on how this should be achieved, most respondents agreed that data sharing forms a necessary part of the future of open banking as a way to deliver consumer protection, innovation and competition. The evidence identified two broad thematic priorities:

#### *Additional data sets*

There was widespread support for an expansion of open banking towards open finance, including not only adjacent products such as savings and loans but also investments and pensions. Such support came particularly from TPPs and expert advisers, and also from some ASPSPs. There was also support for opening up access to non-open finance data sets such as identity attributes. This expansion was seen as a key contributor to enabling innovation and addressing exclusion, whilst also delivering good outcomes for consumers, including the vulnerable, and small businesses.

Reciprocity, whereby firms can only receive data if they also share it, was mentioned as a possible mechanism to encourage sharing, both within and across product markets, and has been a driver of expanded data sharing in some jurisdictions, such as Australia.

#### *Data sharing infrastructure*

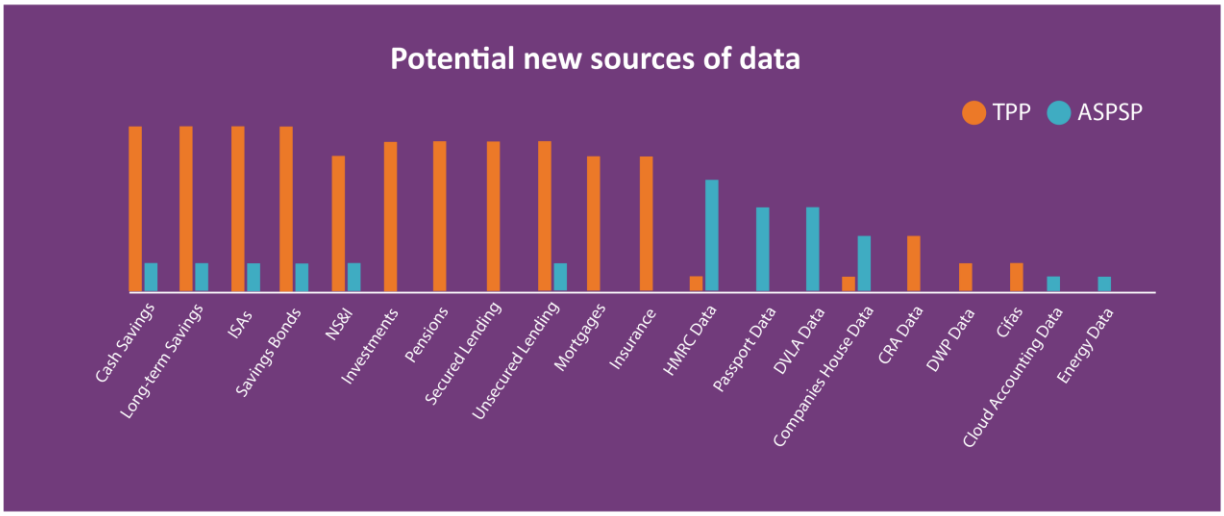
This area refers to evidence provided by many TPP and independent respondents, that there is a need to get the basics of open banking data sharing right by delivering higher standards of reliability and customer experience, providing users with appropriate tools to understand and control their data sharing, and ensuring that open banking delivers for all sectors of society including vulnerable customers. Expert advisers highlighted the growing criticality of open banking reliability, especially in the small business market where down-time and non-availability have a particularly damaging impact.

### 1.5.2. Possible Actions and Prioritisation

There is substantial alignment around the potential for using enhanced data sharing to help reduce fraud and the benefits of “levelling up” the performance of all ASPSPs to the standards of the CMA9, and some alignment on the need to examine ways to improve consumer transparency and control.

There is however significant divergence regarding the sharing of potential additional data sets (see below). In TPP responses the focus was predominantly on expansion initially into adjacent financial products, including savings and investments, which would provide TPPs with a holistic view of a consumer’s financial situation. Banks, on the other hand, identified access to sources of government held identity attributes as more import. This information could be used to improve onboarding, verify identity and reduce fraud.

***Figure 1: Potential New Sources of Data***




Views also diverged regarding the current level of ecosystem reliability and, as a result, a lack of consensus on actions that could be taken to improve matters. To accurately reflect the range of views from stakeholders, we have set out possible actions and areas of prioritisation under three timescales – short-term, medium-term and long-term.

## *Short-term priorities*

**Detailed evidence collection**

The responses received identified that better, and more granular, evidence needed to be collected from across the ecosystem, i.e., ASPSPs and TPPs, to aid policy makers and regulators in their decision-making. Respondents suggested that data is required on standards adherence, API performance and availability, and customer journey completion rates.

**Vulnerable customer propositions**

There was limited evidence of effective open banking propositions aimed at vulnerable customers, primarily due to a lack of commercial return and viable commercial model. However, there was agreement in the benefits of doing so with a wide range of ideas for further work to be undertaken, under three main themes, with many suggesting setting up an industry working group that would:

- Work with charities and consumer groups to undertake research with people with lived experience of vulnerability. This research could also be incorporated into the FCA Financial Lives Survey.
- Explore and understand the reasons for withdrawal of services aimed at vulnerable groups.
- Investigate the potential of sandbox environments (regulatory or digital sandboxes) to help firms develop new services with vulnerable customers in mind.

**Improving reliability and consistency**

Many TPPs and a few other respondents felt strongly that there was still substantial work to do to improve the foundation layer of open banking, before extending to other data sets. Potential actions proposed included:

- Broadening the scope and level of conformance monitoring across all ASPSPs, and focus on improving conversion rates, customer journey consistency and technical reliability.
- Delivering more helpful and precise information through more consistently implemented and more granular error codes (while recognising many banks' concerns about fraud, GDPR and AML risk).
- Speed up and improve the process for evolving the Standard to the needs of the market.

**Data sharing to prevent fraud and prevent exclusion**

In addition to the proposed actions referenced earlier concerning APP fraud, there was also significant cross-stakeholder alignment on the potential benefits of using open banking data to prevent both payment and other types of fraud. This included providing additional account and/or identity attributes in the API, which could also have the positive consequence of improving access to financial services for underserved sectors.

## *Medium-term priorities*

**Exploring forms of MLAs**

The evidence provided suggested a few possible mechanisms through which firms could work together to enable a wider range of data sets to be shared than is currently required.
Such mechanisms ranged from voluntary Codes of Conduct or rule books through to more sophisticated contractual MLAs, although many submissions were sceptical that progress would be made without some form of regulatory mandate.

The Secretariat considered that a phased approach, with each phase building on the previous phases' foundations and learnings, may be an appropriate and constructive way to represent the options suggested by respondents. However, it was clear that many respondents also considered that these phases would need to be accompanied by regulatory intervention. A number of respondents highlighted that markets which had made the most progress in opening up data sharing had been those with clear regulatory mandates.

The phases of such an approach could be:

**Phase 1: Code(s) of conduct or rule books**

- Development of code(s) of conduct or rule books which all participating firms voluntarily agree upon. It was suggested that this might be an appropriate solution for products adjacent to bank payment accounts, e.g., savings, where a relatively limited set of technical changes would be required.
- Early phase activity could be supported by enabling a test environment (such as a regulatory sandbox or a digital sandbox), so that groups of firms could work together to better understand the potential customer impact based on data and, if necessary, make changes to the design of the code or rulebook.

**Phase 2: MLAs**

- Whilst more complex, many respondents suggested that a contractual approach would be required for sharing of more complex data sets such as investments. Such MLAs could cover issues such as liability, standards conformance, API performance and availability, customer protection and inter-firm remuneration (if applicable).
- These MLAs would also ensure that end user interests are appropriately prioritised and be open to external scrutiny and challenge. Some respondents noted that wider data sharing could be encouraged if such MLAs included some reciprocity principles, in order to incentivise the provision of additional data from a wide range of providers across sectors.

**Transparency and control**

Some ASPSPs and most expert advisers suggested that open banking would only be able to scale if it successfully addressed the issue of onward sharing (i.e., providing the user with clear information on what data had been shared by the regulated TPP to whom, and enabling the user to easily invoke their rights to cancel permissions). The two main solutions proposed in this regard were:

- To enhance the visibility of onward shared parties in consent journeys and on banks' access dashboards.
- Improve (and potentially, subject to regulatory agreement, mandate) TPPs' consent dashboards.

A minority of views went further, calling either for the regulatory perimeter to be expanded to include parties receiving open banking data, or for regulated AISPs to be considered data custodians, with a responsibility for monitoring and reporting on the activities of the firms it onward shares data with.

### *Long-term priorities*

**Integration with Open Finance and Smart Data framework**

Many respondents noted that it would be helpful for future data sharing developments in open banking to have a clear pathway to open finance and progressively align to the strategic work being undertaken by the Government on developing Smart Data. The importance of maintaining momentum for the delivery of long-term objectives was referenced by many respondents.

**Alignment with Digital Identity infrastructure**

Whilst there were divergent views on the extent to which digital identity (and, in particular, identity attributes) should be one of the considerations in developing open banking, there was broad acceptance that activity needs to align with the framework being put in place by the

Department for Digital, Culture, Media & Sport (DCMS) and other stakeholders. Many respondents recognised that the wider the reach of open banking, open finance and smart data, the more important it will be to resolve digital identity related issues.

## 1.6. Ensuring a sustainable open banking ecosystem

### 1.6.1. Clarity of Vision and Ambition to Act

Many respondents felt that it was difficult to determine what the roadmap might be without clarity on the vision for open banking, with a number seeking more guidance from regulators about their vision and the outcomes that they wanted to achieve. It was clear from responses that there were differences amongst participants' ambition for the development of the open banking ecosystem. Typically speaking, TPPs were more expansive in their ambition, that dovetailed with the Government's broader agenda regarding Smart Data, compared with that of ASPSPs. However, this was not universally true with individual views falling across a broad spectrum. Maintaining the UK's international standing as a leader in open banking and a global hub for fintech was also mentioned many times.

### 1.6.2. Ecosystem-wide Priorities

This area refers to ecosystem level priorities, typically across both payments and data, proposed in evidence to drive conformance, security, trust, adaptability and good outcomes for end users.

Whilst there was alignment regarding the need for a more proactive approach in developing the ecosystem, not all participants were aligned on which specific activities should be prioritised or the most appropriate way to achieve desired outcomes. These priorities are therefore set out based on areas which had broad based but not unanimous support. These areas are also closely inter-connected with the priorities set out on the Payments and Data sprints.

#### *Conformance & Performance*

This was an important topic in both the Payments and Data sprints, as it was for the ecosystem stakeholders. Several participants set out clearly how greater adherence to the Standard and improved performance would drive increased levels of end-user trust and adoption, as well as enabling TPP propositions to come to market more easily and enabling such propositions to better serve customers. Many submissions reflected on the inconsistencies in the market between CMA9 and non-CMA9 banks, but in aggregate the evidence called for the performance of the whole market to be enhanced.

There was not, however, clarity on how such conformance should be driven, with some submissions suggesting a Future Entity could take on monitoring and conformance powers, others suggesting regulators could perform this function and others suggesting that market forces alone could drive the required improvements. Resolving this emerges as a key question for the Committee to consider as it relates to the functions and structure of the Future Entity or entities.

#### *Trust and awareness*

Consistency and transparency emerged as key levers to improve trust, but a few submissions went further. On awareness, there was limited appetite for a fully-fledged end-user marketing campaign. However, there were a few submissions that suggested that more focused campaigns and communications to promote the awareness and adoption of open banking are warranted, leveraging the support of Government.

An effective disputes system was also critical to driving trust in the responses received, even if there was not clarity on whether disputes should be managed through a centralised system or through a decentralised, point-to-point structure guided by a high-level rule book to guide participants on 'grey area' liability questions. The final aspect of trust which was identified in evidence was the importance of security and resilience of the ecosystem.

### *End user outcomes*

Although many industry participants did not focus on this area, it was emphasised very clearly in submissions by expert advisers, who considered it essential that there was ongoing tracking and monitoring of whether open banking was delivering good outcomes for end users and any risks or detriment was being identified and effectively responded to. A number of responses for example highlighted the importance of considering not just the positive benefits for users of open banking but also considering any negative impacts such as exclusion from those who don't adopt or those who are not digitally included.

### *Evolving the Standard*

Once again, this priority emerged in both the Data and Payments sprints, but there was a broad agreement that the Standard should develop in line with the market and the evolving needs of participants and end users. This should be a key function of the future custodian of the Standard, to prevent splintering of open banking and proliferation of functionality outside the Standard, whilst ensuring that it evolves to reflect changes in the market.

### *Long-term alignment to broader initiatives*

Evidence was consistent that the evolution of open banking needs to dovetail with broader initiatives. In Payments, a common theme was the need to integrate the longer-term vision with the NPA and broader strategy for the evolution of UK Payments. In data, there was powerful evidence about the need to integrate open banking data sharing with the evolution of open finance and Smart Data. Several submissions referred to the importance of the UK maintaining its position as a global leader in fintech and suggested that without visionary thinking and a clear evolution from the current state to a future industry structure this position could be lost.

## 1.7. Future industry structure

### 1.7.1. Successor Entity to the OBIE (or "Future Entity")

A broad range of views were submitted regarding the future structure of the ecosystem to support the successful development of open banking. There was a general view that some form of successor entity (or entities) to the current the OBIE would be required, although there was limited agreement on the nature, scope or authority of that entity (or entities). There was, however, a strong preference from many stakeholders that the Future Entity (or entities) should assume the role of a central standard setting body to develop and maintain future Open Banking Standards, with respondents seeing a potential role of the Future Entity as a standards centre of excellence with a broader remit than open banking, thereby supporting the development of long-term open finance and Smart Data capabilities and digital financial infrastructure for the UK economy. A number of ASPSPs highlighted the importance of setting up a Future Entity and felt it should be the first step in the further development of open banking.

It was also highlighted by a range of submissions, that the Future Entity should have a clear remit to focus on the needs of consumers and small businesses, and to ensure that their views are effectively represented in its governance.

### 1.7.2. Core Activities

A strong emerging theme from the evidence was that certain services should be seen as core to the future development of open banking, which for practical reasons need to be provided centrally. Examples provided by respondents regarding these essential activities were:

> Maintaining the Open Banking Standard to ensure it stays relevant.
> Collecting and collating MI, and obtaining additional evidence to help decision-making.
> Monitoring standards conformance. However, there was some divergence as to whether the Future Entity would provide evidence and outputs to regulators or if it would be given powers to enforce adherence and conformance on participants.

### 1.7.3. Non-Core Activities

Beyond these core activities there are some support services, currently delivered centrally by the OBIE which, although they may be essential, could be delivered in alternative ways. Examples suggested by some respondents included:

> Trust services, e.g., entity identity certificates and permissions checking.
> Implementation support.
> Ecosystem promotion.

There were considerably divergent views as to how trust services could be delivered in future. Some respondents felt that how this framework is delivered – currently, via the OBIE's Open Banking Directory – should be reviewed, and that alternative delivery models may improve resilience, scalability, and be more affordable, for example trust services could be delivered to an agreed Standard by a number of providers as demonstrated in other jurisdictions. TPPs were not averse to change but cautioned that any changes may risk disruption to the market and any

potential disruption had to be carefully managed. A key principle that many respondents supported was that the Future Entity should only support activities that cannot be provided by the market.

### 1.7.4. Possible Model

Interpreting evidence presented, a possible model for the Future Entity is that its role is limited to the provision of a limited number of core services i.e., standards development, MI collation and conformance monitoring, with other services being delivered in a variety of ways, i.e., by the Future Entity, by another entity (or entities), or via the market. This approach would potentially deliver a single focused, centrally governed and funded standards body which could be scalable into a centre of excellence for standards development, spanning cross-sector open data initiatives. Harmonisation across implementations and reducing costs of scalability (e.g., when moving from open banking to possible open finance use cases) was considered by many respondents as sensible and desirable. Some ASPSPs recommended the rapid transition of essential 'core activities', and the prioritisation of an assessment of how best to disperse or discontinue non-core activities, such that they do not become embedded in and encumber the Future Entity.

### 1.7.5. Alternative Models

A few respondents envisaged that a Future Entity might continue to deliver centralised services, such as Directory services, as currently provided by the OBIE. However, this was a minority view and several stakeholders cautioned against this approach, particularly if the entity were to take on a broad role with a wide range of responsibilities, which might have complex implications for funding, liability and governance arrangements.

A very small number of respondents did not believe a Future Entity was needed. However, this was opposed by many respondents on the basis that it would result in a highly fragmented ecosystem leading to lower consumer and SME adoption, and the potential marginalisation of open banking use cases and developments.

### 1.7.6. Funding

Respondents generally noted that it was challenging to precisely determine the optimal funding model without knowing what services the Future Entity will provide to deliver for what kind of open banking future. However, there was strong agreement that the development of a sustainable funding model, requiring contributions from a wide pool of industry participants, is required. Although there was further alignment to the principle that any funding model needed to be fair and equitable, there was limited detail regarding how that could be achieved.

Funding options such as membership fees, regulatory levies and pay per usage fee were featured, but there was no consensus on an optimal approach or even the extent to which different funding methods might be appropriate for each of the Future Entity's activities. Some stakeholders suggested a mixed source and mechanisms of funding would be necessary and represent a constructive way forward. A few respondents considered that these activities should be publicly funded given the importance and potential of open banking for the wider UK financial system and the economy.

A few expert advisers noted that any future funding approach needed to ensure that there was no correlation between the level of funding and funders' influence on the future direction and strategy of the Future Entity. Some also highlighted the importance of ensuring that the interests of consumers and SMEs were prioritised under any future governance structure.

# INTRODUCTION

## 1.8. Background

The Joint Regulatory Oversight Committee ("the Committee"), the cross-authority taskforce responsible for the oversight of open banking in the UK, set up a strategic working group (SWG) in August 2022. The purpose of the SWG process was to bring together industry and other stakeholders to provide the Committee with expert input into the vision and strategic roadmap for further developments in open banking.

The Committee's co-chairs, the FCA and the PSR, appointed Bryan Zhang[3] as the Independent Chair of the SWG and asked the OBIE to act as secretariat and provide administrative support. The Independent Chair worked in consultation with the Committee to appoint members to the SWG and expert panels (on data and payments), representing open banking ecosystem stakeholders, end users, and expert advisers (see Appendix 2 for a full list of members). A series of open banking strategy sprints were held with the members of the SWG and expert panels from early September to late November 2022.

## 1.9. Objectives of the SWG

The Committee initiated the SWG process to:

1. Collate views and input from industry and broader stakeholders into the vision and strategic roadmap for further development of open banking. This includes consideration of the priority areas outlined in the Joint Regulatory Statement:
    - Unlocking the potential of open banking payments such as through account-to-account retail transactions.
    - Enabling end-users to share data and manage access with trusted third parties.
    - Developing further data sharing propositions, including for consumer protection.
2. Provide the Committee with stakeholders' views on the priorities, long-term governance, and funding options for the Future Entity, to ensure it is set up, resourced, and funded on a sustainable and equitable basis for the future. (The "Future Entity" is the term used to refer to an appropriate successor to the Open Banking Implementation Entity).
3. Provide views to the Committee on what activities should be taken by the Future Entity and whether activities should be taken forward by organisations other than the Future Entity to achieve the desired objectives.
4. Address any other requests the Committee might have.

[3] FCA announcement 9 August 2022 and PSR announcement 9th August 2022

## 1.10. Methodology – collecting evidence

The Independent Chair of the SWG, in consultation with the Committee, decided to gather data through two series of virtual thematic "strategy sprints", each focusing on one of three key areas:

1. **The Payments Strategy Sprint: unlocking the potential of open banking payments.**
2. **The Data Strategy Sprint: promoting further data sharing in an open banking framework.**
3. **The Ecosystem Strategy Sprint: ensuring a sustainable open banking ecosystem.**

Expert Panels were set up to carry out the Payments Strategy and Data Strategy Sprints, whilst the SWG members conducted the Ecosystem Strategy Sprint themselves. The Committee provided a set of questions for each sprint, with Panel Members (for Payments and Data Strategy Sprints) and SWG members (for Ecosystem Strategy Sprint) encouraged to submit evidence-based written responses. General submissions from the full range of open banking participants were also invited. Panels met at the commencement of each Sprint which culminated in a two-hour panel session on Microsoft Teams, with minutes of each session published on the SWG website[4].

The SWG website includes the full list of questions[5] set by the Committee and the list of SWG and expert panel members (please see the full list of members in Appendix 2).

The first series of strategy sprints were conducted in September and October to answer the first set of questions set by the Committee. The focus of the first sprint was to identify potential gaps between the current state of open banking ecosystem and a more optimal state in the future.

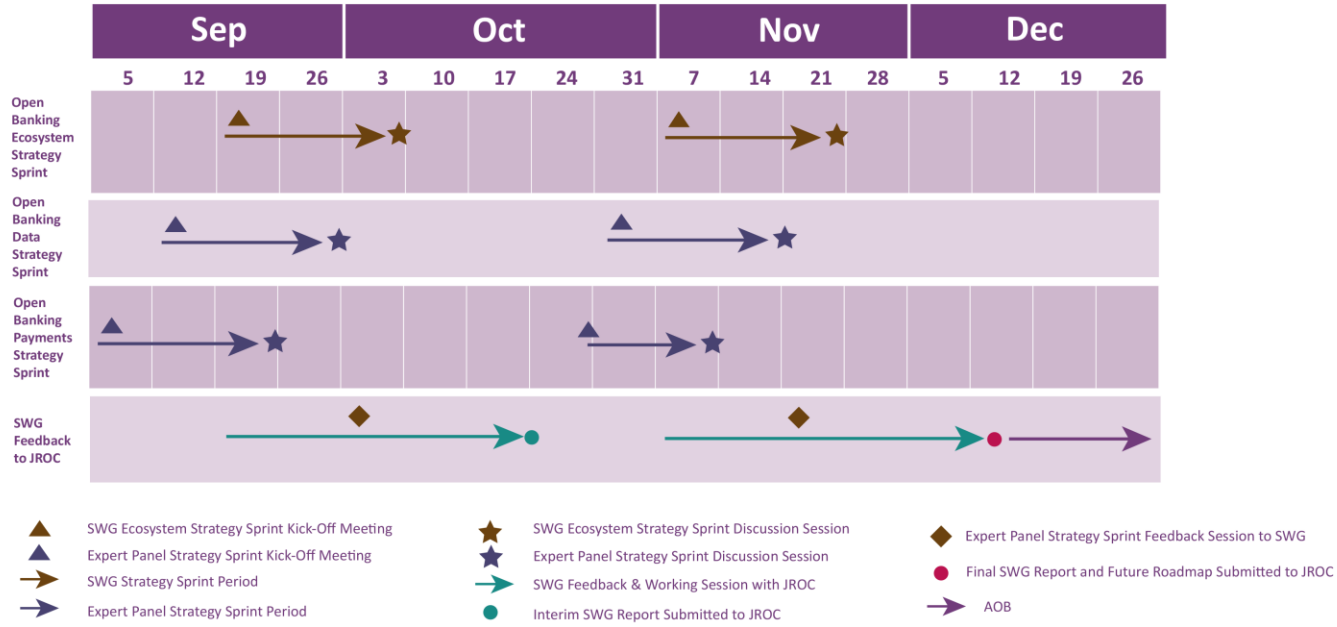
A second series of sprints, based on a new set of questions from the Committee, was conducted in November and December and has been considered together with the findings of the Interim Report, published on 14 October 2022. The focus of the second sprint was to identify what further evidence is required to assess the state of play today; what activities should be prioritised and what actor(s), including regulators and the Future Entity (or entities) should play what kind of role in operationalising the priority issues.

A Draft Final Report, based on the evidence gathered from both series of sprints was issued to the Committee, the SWG and members of the Expert Panels on 21 December 2022. Feedback was received from the Committee and 14 respondents.

Informed by the feedback received the Secretariat issued this Final Report for the Joint Regulatory Oversight Committee in February 2023.

[4] https://www.openbanking.org.uk/swg/
[5] https://www.openbanking.org.uk/wp-content/uploads/JROC-Questions-.docx

**Figure 2: Timeline and milestones of the SWG open banking strategy sprints**



## 1.11. Engagement

In total, the SWG Secretariat received 189 pieces of written evidence from 104 different organisations, and 88 people representing 71 institutions attended the SWG and panel sessions. In addition, 100 people representing 89 institutions attended two public SWG information sessions. Table 1 below provides detail of written submissions received and the composition of respondents.

**Table 1: Number of submissions received for each sprint**

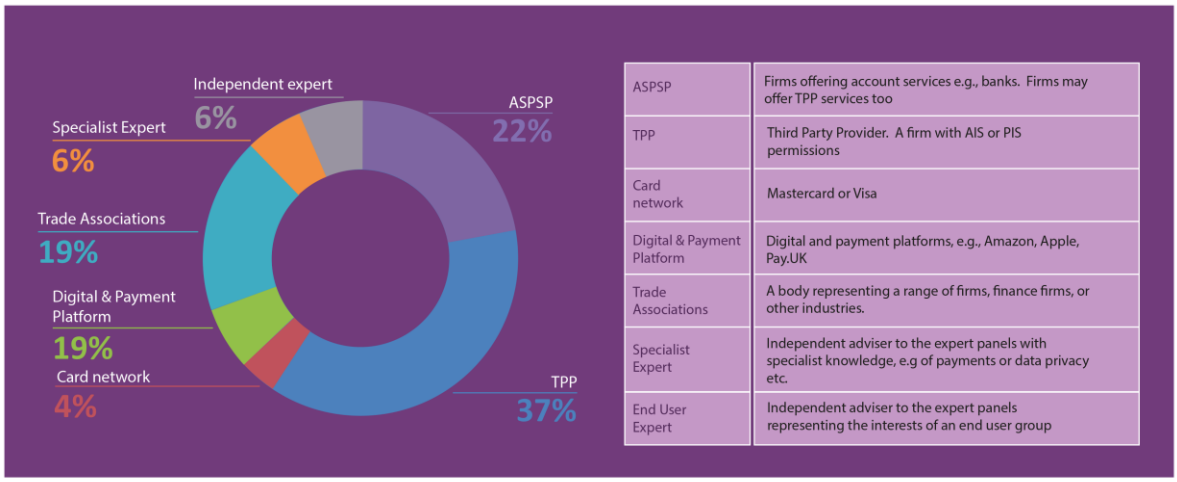
| | Sprint Round 1 | | | | Total | Sprint Round 2 | | | | Total |
|---|---|---|---|---|---|---|---|---|---|---|
| Category | Payments | Data | Ecosystem | All | | Payments | Data | Ecosystem | All | |
| Panel member submissions | 26 | 28 | 16 | - | 70 | 20 | 25 | 12 | - | 57 |
| General submissions | 11 | 6 | 16 | 6 | 39 | 6 | 5 | 9 | 3 | 23 |
| Total | 37 | 34 | 32 | 6 | 109 | 26 | 30 | 21 | 3 | 80 |

| | | | |
|---|---|---|---|
| Total submissions | 109 | 80 | 189 |

*Note: The Strategic Working Group undertook Ecosystem Strategy Sprints.*

Written submissions were received from a wide range of respondents representing all sections of the UK open banking ecosystem as demonstrated in Figure 3 below:

***Figure 3 – Range of respondents***




*Note: To ensure participant confidentiality is maintained in the report, card networks and digital and payment platforms are collectively referred to as platforms and specialist experts and end user experts are collectively referred to as expert advisers.*

## 1.12. Analytical Frameworks

For the first round of sprints, a common analytical framework was employed consistently to examine and analyse the evidence collected through written submissions and to facilitate strategy sprint discussion sessions. This framework was underpinned by gap analysis to identify key issues, or "gaps", between the current state of open banking and a more optimal state in the future. These include:

- **Gaps which affect the decisions of providers and potential providers of services to create and enhance customer propositions.**
- **Gaps which influence consumers and businesses to adopt or continue to use open banking-based propositions.**
- **Gaps in the support aspect of the customer journey, including what happens when something goes wrong.**

Through 109 written submissions received in the first sprint, respondents identified a wide range of gaps which are summarised in this report. We also examined how different stakeholder groups might perceive these gaps differently, resulting in 'gaps of perception' on certain key issues. Where relevant, we have also employed a 'consumer-centric' lens to consideration of the issues, particularly consumer choices, experience, and protection.

The focus of the second round of sprints was on the vision for open banking, its evolution towards open finance and A2ART and how to 'operationalise' a variety of activities. The analytical framework employed in this sprint was based on a combination of thematic prioritisation, consideration of sequencing, responsibilities for implementation and potential timescales of activities, identified from the written evidence that was collected. Short-term was defined as 12 to 18 months, with long-term recognised as being more than 18 months, in line with the guidance issued by the Committee.

It should be noted that whilst a significant volume of evidence was received in relation to the first round of sprints, to highlight and quantify specific gaps, the availability of empirical data concerning future approaches to addressing gaps was much more sparse and inevitably most responses to this part of the process were opinion-based.

In addition to the work of the Secretariat in summarising and synthesising the evidence and views presented, the Committee had direct access to a wide and representative range of first round submissions, and all non-confidential second round submissions (confidentiality provisions were amended between sprints).

## 1.13. Constraints

A minority of respondents raised concerns relating to the process and noted that the ambitious timetable for the sprints and lack of time to gather data had hampered their ability to contribute evidence. They noted that this may have resulted in inputs based more on opinion rather than empirical data, which may not necessarily provide a sound basis to determine what new functionality or improvements are necessary or desirable for the ecosystem.

It was further noted that, despite the involvement of independent consumer and small business experts in the process, a limitation of the methodology was that the views of the end users of open banking-enabled products were not directly sought. A small number of respondents questioned the scope and structure of the questions set by the Committee, and expressed concerns that some important issues in their view, were not satisfactorily covered.

Neither the SWG nor the Secretariat were in a position to make specific recommendations pertaining to the future roadmap of open banking to the Committee per the mandate of the SWG, as defined in its Terms of Reference.

# KEY FINDINGS FROM THE STRATEGY SPRINTS

## 1.14. Summary of findings from Payments Strategy Sprints

The Payments Strategy Sprints were focused on collecting evidence to enable the realisation the Committee's objective of "unlocking the potential of open banking payments". Payments Sprint 1 focused on identifying several key gaps between the current state of open banking and realising the stated ambitions for the future. Sprint 2 focused on exploring priority initiatives to realise this objective. Whilst there were many areas of debate in the process, some broad conclusions and choices can be drawn out for consideration by the Committee. These are structured around the four key gaps identified in Sprint 1 and the three key priority areas identified in Sprint 2.

### 1.14.1. Key Gaps Identified

#### *1.14.1.1. Gap 1: Underpinning Data*

There was a general aspiration to progress open banking payments and work towards the realisation of the vision set by the Committee. However, participants suggested that objective and reliable data on the performance of the open banking payments ecosystem on important topics such as fraud levels, conversion rates and API availability would help to make better decisions on the way forward. Whilst individual participants submitted powerful data, without any ability to verify or cross-reference it was hard to draw firm conclusions across the open banking ecosystem, particularly as much of the data was contradictory. For example, a few ASPSPs submitted data showing that fraud levels were higher on open banking payments than other channels, a view challenged by TPPs. TPPs on the other hand submitted data which showed low conversion rates, particularly for higher value transactions.

#### *1.14.1.2. Gap 2: Customer Choices*

Most respondents supported development of open banking payments in line with the broad vision set by the Committee, but recognised that there were three important gaps that prevent merchants and other beneficiaries from adopting open banking payments at scale.

The first area of note was functional gaps. Whilst many proposed technical enhancements were provided in evidence, the most consistent case was made around functionality to enhance the level of certainty as to whether the payment was executed, the status of the payment or why it had failed. The other critical area of requested functionality was extending VRPs to non-sweeping use-cases, which was championed by TPPs, but not by many ASPSPs.

The second area related to performance. There was substantial evidence from across the ecosystem, in particular from TPPs, that the levels of payment conversion, reliability and resilience will need to be higher to enable more payments use-cases to be viable.

Third, there was evidence that an asymmetry of costs and incentives within the ecosystem was a fundamental impediment to an expansion of open banking payments into areas such as e-commerce, broader Account-to-Account Retail Transactions ("A2ART") and non-sweeping VRPs.

#### *1.14.1.3. Gap 3: Customer Experiences*

As well as the barriers to adoption by merchants, Sprint 1 also identified barriers to broader adoption of open banking payments by consumers and small businesses for high value transactions.

The main gap identified in this space was that the level of reliability and successful completion was too low, particularly for high value transactions, which in many cases were restricted. Many ASPSPs in their submissions provided evidence that legitimate fraud prevention measures and payment limits necessitated stopping or investigating many transactions, but TPPs provided some compelling evidence about the impact that this was having on the customer proposition.

The effect of this, irrespective of the cause, is that many high-value open banking payments get declined and additional frictions can enter the journey, such as extra screens or calls. One TPP mentioned that new payee limits – and for many e-commerce use-cases most payers have no existing relationship with payees – were capped as low as £2,000 in the case of one large UK bank. Given that the underlying economics of open banking payments is more favourable to TPPs with high-value payments use-cases, this is a substantial issue.

#### *1.14.1.4. Gap 4: Customer Support*

Sprint 1 identified two critical gaps in terms of supporting customers using open banking payments, both related to issues when things go wrong and ensuring that the ecosystem has the right rules and processes in place.

The first gap which most ASPSPs and expert advisers identified related to effective customer protection – in particular, regarding some retail transaction types – that could expose payers to detriment and undermine trust in open banking payments. Evidence was contradictory here, with many respondents including expert advisers and banks arguing additional protection is essential for open banking payments to succeed. TPPs and many retailers, however, argued that this would add cost, complexity and hold back the development of open banking payments. A useful distinction was drawn during discussion sessions between payment disputes and purchase disputes. Payment disputes (for example, payment errors, payment not authorised) are not frequent and existing mechanisms and regulation were described as sufficient today. Purchase disputes (for example, where goods are not received, or a supplier goes out of business) are where the key gap was identified by some participants.

The second gap related to dispute-handling in terms of rules and systems. One of the challenges was predicting the volume and type of disputes that the open banking ecosystem will generate as it grows and develops. Evidence highlighted that the volume and type of disputes will also be impacted by decisions relating to purchase protection, and therefore these gaps are very closely connected. For example, a broader customer protection regime will inevitably generate a higher volume of disputes, as seen in the chargeback process in the cards ecosystem. A narrower customer protection regime will generate less disputes.

### 1.14.2. Potentially Prioritised Initiatives

#### *1.14.2.1. Prioritised Initiatives Theme 1: Fraud and Friction*

Approximately 70% of submissions supported a Future Entity collecting, verifying and publishing data on fraud, conversion and overall performance to enable clear decision-making on this complex and nuanced topic, and to provide a consistent fact-base for the ecosystem. Conversely, a minority of

respondents suggested a regulator should play this role, or an industry body like UK Finance. There were some calls for the data to be published at firm level, but most supported data being published at an aggregated and anonymised level. 70% also stated that data should be published for both ASPSPs and TPPs. Some responses highlighted an important consideration: effective, whole of market data collection is likely to need some form of regulatory mandate.

Despite the conflicting evidence on this topic, there was broad acceptance that this was a priority area to resolve. When analysing priorities supplied as part of Sprint 2, this area emerged as a key priority for ASPSPs and TPPs alike. Only two large ASPSPs suggested that this was not an important area of activity.

In the short term, there was broad support for deploying TRIs as an effective solution to address the issue of fraud, provided that these are accurately completed for all transactions for all PISPs and used as part of risk scoring by ASPSPs. Most submissions supported the expanded use of TRIs, with a minority suggesting that to be effective their use would have to be mandated. No submission opposed the adoption of TRIs.

Some respondents argued that the effective implementation of TRIs could resolve some of the issues on payment limits, which were of considerable concern to many TPPs. Richer transaction-level risk information would provide an improved alternative to blunt anti-fraud measures such as transaction limits. TPPs were highly supportive of solutions that address the issues that the application of payment limits currently cause.

Longer term, a few submissions considered more far-reaching solutions to the challenge of reducing friction without enabling greater levels of fraud. Whitelisting certain destination accounts was suggested by two submissions, but most considered that the ultimate solution probably lay in the sharing of liability in some way between ASPSP and TPP. This, it was argued, will likely require some form of contract, ideally an MLA, given that bilateral contracts have typically been identified in evidence as:

- **Inefficient – participants need to negotiate arrangements on an individual basis which is time-consuming;**
- **Potentially discriminatory – smaller players have considerably less negotiating power and can be excluded from market participation or afforded considerably less favourable terms; and**
- **Insufficiently transparent – not enabling participants to see how rules are implemented across the market and ensure equitable treatment in decision-making and peer review.**

#### *1.14.2.2. Prioritised Initiatives Theme 2: Improving Ecosystem Performance*

On payment functionality, Sprint 2 confirmed that the areas of greatest short-term potential related to payment status and error codes. There was broad support for undertaking more work in this space. Beyond this, many submissions considered that most other functional enhancements, whilst of clear value and potential to drive adoption, should only be considered in the context of the NPA but this need not delay the short-term initiatives. This underlined the importance in evidence of working closely with Pay.UK on longer term payments strategy, particularly when considering additional payments functionality required to address new market segments.

A few respondents highlighted the importance of assessing true demand for new developments / capabilities including testing with real customers, for example by using the regulatory sandbox, and/or leveraging a digital sandbox which utilises synthetic data.

On the issue of protection, most banks and expert advisers favoured a strong protection regime and most TPPs and retailers preferred to rely on the existing PSRs, sector-specific schemes such as ABTA and the Consumer Rights Act to protect customers. Responses were either in favour of comparably consistent protection, broadly equivalent to cards; or were opposed to replicating card-style protections, seeing it as unnecessary or too complex. There was some nuance in responses, however. Some submissions saw protection as important but considered that the market could solve the issue. Others distinguished between types of protection and suggested that bankruptcy protection should be offered but other types not.

The question of disputes saw more common ground, with most responses seeing this as an important topic to resolve and ensure that the future ecosystem had an appropriate model to deal with disputes. This was identified in responses from retailers as essential. The exact nature of this solution and whether it should be centralised or decentralised was not clear in submitted evidence. It did emerge as an area where additional work to scope and define options would be of value, with the potential for the creation of a code of conduct / rulebook to assist firms dealing with disputes. This code of conduct could additionally address consumer protection issues if common ground can be found.

#### *1.14.2.3. Prioritised Initiatives Theme 3: Expansion of VRPs beyond sweeping*

Most respondents saw some potential for a short-term expansion of VRPs into low-risk or lower risk sectors such as government, charity, utilities and regulated investments. However, most were clear that any longer-term expansion would require some form of intervention in terms of a regulatory mandate, an MLA or regulatory actions on pricing (e.g., a price cap) and liability model. Some considered that the market would solve such issues in time, but these views were in a minority. Expert advisers also highlighted the importance of consumer protection. It was generally suggested that one of the responsibilities of a Future Entity could be the creation of an MLA to support the orderly expansion of VRPs beyond sweeping.

Whilst some evidence on inter-firm remuneration was provided, typically from TPPs concerned that it would lead to insufficient returns unless capped or fixed at zero, several submissions considered it inappropriate to discuss pricing matters, and that should be left in the commercial domain. However, there was wide agreement that the current commercial realities are unlikely to lead to the expansion of VRPs, especially in the short term.

## 1.15. Summary of findings from Data Strategy Sprints

The data strategy sprint focused on the vision for open banking and open finance, to realise the Committee's objective of, "empowering consumers and SMEs further through more informed choice and a broader range of financial services tools and products by promoting further data sharing propositions." The first sprint focused on identifying a number of key gaps that evidence suggested would act as barriers to realising this vision.

The second sprint focused on exploring the extent to which activities to address these gaps should be prioritised and which actor(s), including regulators and the Future Entity, should play a role in operationalising the priority issues. Whilst there were many areas of debate in the process, some broad conclusions and choices can be drawn out for consideration of the Committee.

### 1.15.1. Key Gaps Identified

#### *1.15.1.1. Gap 1: The role of data sharing to prevent fraud*

In sprint 1 respondents generally agreed with the benefits open banking could provide in terms of sharing data to reduce fraud. However, there was a fundamental divergence between banks and TPPs as to the quantum of new fraud risk introduced by open banking payments. This divergence was at the root of differing perceptions of how providing additional data elements could improve fraud detection and ultimately consumer outcomes.

ASPSPs were aligned in their views that the TRI data points included in the Open Banking Standard were the right ones, whilst recognising that fraud attack vectors continuously evolve. They were keen to test their effectiveness before looking to extend them to include additional data points. Their justification was not only a desire to effectively use existing data but to also adhere to data minimisation principles.

The main concern expressed by all banks and some TPPs relates to how widely TRIs will be implemented and used. Effective use of TRIs by all participants relies heavily on mutual incentives to reduce fraud and reduce false positives by more intelligently risk-scoring transactions using predictive data. Some large ASPSPs are mandated under the CMA Order to be able to receive prescribed TRI fields but are not compelled to use them. The Standards are not mandatory for TPPs. All the ASPSPs that responded considered that rules, whether via MLAs or regulatory intervention, would be required to achieve this.

The majority of TPPs identified several additional customer attribute data points that would improve their own risk scoring. However, some TPPs and all the banks questioned whether TPPs can realistically play a key role in fraud detection given the disparity in the information available to them compared to banks, in particular on customer payment behaviour patterns that help detect high-risk transactions. The current TRIs are mono-directional from PISP to ASPSP.

The API-based Enhanced Fraud Data Solution (EFDS) being developed with UK Finance was widely referenced by ASPSPs. Good evidence was provided that the data components that it is intended to exchange would enable material improvements in authorised payment fraud detection for inter-bank payments. It was suggested by ASPSPs that it would be prudent to wait until this initiative is delivered before considering additional measures.

Whilst few respondents identified the difficulty in sometimes identifying the end recipient of data or merchant - for example, on a statement or a dashboard - as presenting a significant ecosystem risk, there was widespread agreement for providing consumers with transparency, for example by ensuring that the final recipient of the data or the payment was clear. There were varying views as to whether the current model to achieve this was fit for purpose, with most TPPs stating that it was not, whilst ASPSPs did not believe there was a strong enough case for change.

#### *1.15.1.2. Gap 2: Sharing Identity Data*

There is significant appetite from the TPP community to consume additional identity attribute data from ASPSPs for fraud prevention purposes. However, there is limited appetite on the part of ASPSPs to obtain such data from TPPs on the basis that the banks typically hold more comprehensive and higher quality attribute data and their preference is instead focused on obtaining government-sourced attribute data.

There is some appetite amongst ASPSPs to provide additional data to PISPs to enhance customer payment experiences by enabling pre-population of information in the payment flow, such as age verification, but this was not an opportunity identified to any extent by the TPP community.

ASPSPs accept that there may be commercial opportunities in providing identity attributes but are not in favour of this being delivered via open banking. The primary reason for this hesitancy is that this is already a crowded space with competing initiatives, some of which are advanced, working within the new DCMS Trust Framework. An additional concern is the reliability of personal attributes held by ASPSPs, particularly as some of their data could be many years old and not captured from a primary source. This lack of reliability could give rise to complex issues of liability.

#### *1.15.1.3. Gap 3: Widening Access and protecting vulnerable customers*

There was broad agreement that open banking data sharing can deliver a range of potentially valuable services for customers in vulnerable circumstances. A considerable number of innovative ideas were referenced, with wider access to credit by enhancing the current Credit Reference Agency data set identified as a possible option, which would be applicable to both consumers and SMEs. Compelling evidence was provided to illustrate that access to affordable credit is still a significant issue and one where access to a broader pool of data could play a key role. Some respondents referenced the positive value of tools and resources to help consumers to navigate the cost-of-living crisis.

It was widely noted that a key limitation of open banking from an accessibility perspective is that only those who are digitally banked can use it. One large ASPSP indicated that c.40% of current account-holders are not digitally active.

A few respondents noted that the commercial viability of many services aimed at vulnerable consumers was a potential barrier to development of these propositions. It was noted that several services had been withdrawn from the market after launch. It was suggested that consideration should be given to publicly funding some of these potentially valuable services.

Evidence was provided that when considering how to meet the needs of vulnerable consumers it was important to work with them to accurately identify their specific needs and ensure that solutions meet them.

Some respondents cautioned that while there are considerable opportunities for open banking to be a positive force for vulnerable people, they may introduce detrimental consumer outcomes. One specific example was referred to in evidence: the possibility that open banking could be used to circumvent gambling blocks widely implemented for card-based payments. Another was the development of an open banking-enabled service to address the challenges faced by communities where bank branches are being withdrawn. It provides bank-agnostic in-branch services - such as cash withdrawals, deposits, payments, and face-to-face support - for people and SMEs in communities where traditional bank branches have disappeared.

It was also noted that open banking could exacerbate exclusion, given the high number of consumers who are not digitally active or who may not be comfortable with sharing their data.

There was divergence on what is needed to accelerate the provision of services designed to improve financial inclusion and support vulnerable consumers. Some respondents consider that these types of services could be delivered on an existing basis using data currently available via open banking. Others believe that it is necessary to extend that pool of data. Some respondents considered that

including savings and loan accounts were essential. Others considered that open banking should be extended to other data sets such as open finance, government and utility company data. Those championing tools that support ways to reduce climate footprints see expansion of data sets as particularly necessary, so that these tools can be expanded to enable more accurate profiling of carbon impacts of activities. For example, tools that can identify transactions relating to transportation, utility consumption and purchasing can be used to track consumer and small business carbon impact of activities and give advice on how to reduce it.

#### *1.15.1.4. Gap 4: Critical capabilities and functions needed to support wider data sharing (including MLAs and additional standards & guidance)*

The majority of TPPs were critical of the quality and performance of the APIs available in the UK market today and believe that improving this is a critical foundational measure to support further data sharing propositions. ASPSPs referenced the OBIE's regular publication of open banking statistics as evidence that there is continued improvement in performance.

There was broad support for an ecosystem-wide monitoring and enforcement regime to ensure conformance, but there was no consensus on the most appropriate mechanism to achieve this. TPPs wanted more consistency across data providers, expert advisers wanted to ensure an open market in which all players could participate irrespective of size and ASPSPs wanted a common and consistent oversight regime.

Several respondents referenced a lack of incentive for data providers to invest in the capabilities required to expand the range data they share with third parties, suggesting that a new regulatory framework will be required to realise the expansion of open banking to open finance.

Some respondents identified a need for additional standards and guidance for data providers not subject to the CMA Order. Others noted that elements of the existing UK Open Banking Standard were optional, which led to inconsistencies. However, there were clear divergences of opinion on the need to enhance different elements of the existing standards and the priority of this.

The absence of specific guidance on data ethics was identified by expert advisers as a gap that will be required to support the expansion of data sharing propositions beyond open banking.

MLAs were identified as a potential mechanism to facilitate data sharing on a commercial basis, but there were divergent views as to how this should be achieved.

### 1.15.2. Potentially Prioritised Initiatives

#### *1.15.2.1. Prioritised Initiatives Theme 1: Expansion of Data Sets*

There was strong agreement that open banking propositions will benefit from increasing the scope and availability of new data sets, but there were clear differences between stakeholder groups on which new data sets would be most valuable. Expert advisers highlighted the competition benefits of opening access to savings; with significant inert balances, TPPs could deliver significant value to customers. Most TPPs considered that all end user-owned data should be sharable via APIs. Their key area of initial focus is on expansion into adjacent financial products which would provide customers with a more holistic view of their financial situation.

Banks on the other hand identified access to sources of government-held identity attributes as of more importance, which could be used to improve onboarding, facilitate identity verification, and help reduce fraud. Several banks stated that they were unclear as to the purpose of expansion of

open banking into savings accounts and questioned whether a regulatory-driven approach to open finance would deliver benefits that justify the costs. In their view, any proposed expansion needs to be built on clear problem statements, identified consumer demand for solutions and a strong cost benefit analysis.

Several respondents including both banks and TPPs suggested that a pragmatic approach to extending access to new data sources would be to exploit existing infrastructure to support access to savings account data. It was noted by several banks and TPPs that existing APIs have been built to support access to such data, but access has not been provided. Some ASPSPs indicated that the legal definition of a "payment account" had prevented access to many savings and other open finance products.

It was suggested that a narrow, project-specific MLA could be developed for prospective participants covering liabilities, dispute resolution and other commercial considerations to facilitate a pilot to test access to savings accounts propositions in a controlled environment. This would allow participants to gather evidence on its attractiveness to consumers, what consumer protections may be required, and the suitably of potential commercial models. This not only allows industry to build a pathway to more extensive MLAs, but also allows the Committee to explore the extent to which the market can achieve desired outcomes or whether additional regulatory intervention is required. This approach could be extended to cover other opportunities over time.

#### *1.15.2.2. Prioritised Initiatives Theme 2: Upgrading Ecosystem*

It was generally accepted by all respondents that there were opportunities for levelling up the performance of the ecosystem, which would lead to more consistent experiences for end users of open banking-powered services. However, there were some differences of opinion as to how this could be achieved. Several respondents questioned whether specific intervention was required now rather than allowing more time for the ecosystem to mature given that it has already shown improvement since inception, and this is expected to continue.

Respondents suggested a range of initiatives that could help upgrade the ecosystem:

**Performance monitoring and reporting**: The action of monitoring and reporting (either to a regulator or publishing) was felt to be a suitable mechanism that would lead to operational improvements. The importance of data collection was highlighted in the Sprint 2 responses and there was a broadly held, but not universal, view that the Future Entity should have an important role in the collection of this data. Several respondents felt that this role would benefit from regulatory support or direction to ensure that the Future Entity had the powers to collect this information from ecosystem participants and provide a broader base than the current levels of MI reporting. Some respondents felt that minimum regulatory targets or KPIs would be needed to ensure performance.

**Appetite for extending standardisation:** A significant number of respondents expressed a desire to extend standardisation across the open banking ecosystem. This covered technical performance of the ecosystem, where TPPs were keen to see mandatory requirements extended across non-CMA9 banks and banks also argued that conformance was needed across all ecosystem participants. Some TPPs also called for mandatory adoption of certain optional components of the existing Standard, such as transaction IDs.

**Support emergence of vulnerable customer propositions:** It was identified in the first sprint that developing propositions that support vulnerable customers has proved difficult from a commercial

perspective. To realise the potential of such propositions, most respondents saw a clear role for regulatory support. There was widespread support for regulatory engagement with charities and other relevant experts to support funding and execution of research with consumers with lived experience of vulnerability. The suggestion of opening new sandboxes or utilising an existing FCA regulatory sandbox or digital sandbox was supported in a few responses. More radical measures were suggested by a few respondents who felt that regulators may need to secure funding and mandate cooperation of participants to achieve the delivery of propositions that would deliver societal benefits, which may not be commercially viable.

**Investigate ways to improve transparency of data sharing:** Many respondents considered that there was a need for greater transparency to help build control and trust for end users when sharing data, including "onward sharing" to other parties. A few respondents called for a restriction of onward sharing. To the contrary, six respondents felt that there were no issues with the way that the onward sharing of data currently works.

Two solutions to improve the transparency of data sharing were commonly identified:

- **Expanding the availability of consent dashboards at TPPs, ensuring that these include onward sharing arrangements and allow end users to understand who has access to their data and stop it if they wish to.**
- **Enhancing the transparency of onward sharing during the initial consent journey and on access dashboards, by sharing the details of the onward sharing party with the ASPSP, rather than relying on the current "software statement" solution.**

A few respondents proposed that the Standard should be extended to provide more guidance and clarity of language in relation to onward sharing or suggested that a 'dashboard of dashboards' concept could help to bring greater transparency, although this did not attract significant support.

**Data sharing to prevent fraud:** The importance of having comprehensive data and robust mechanisms to monitor the incidence of fraud was widely acknowledged by all participants. They noted the risk that as fraud vectors change, existing metrics need to be adapted. Most respondents saw the Future Entity as having primary responsibility for the collation of cross-industry open banking fraud statistics, but respondents noted that opportunities should be taken to align with existing fraud-reporting mechanisms to prevent duplication.

Most respondents were supportive of the development of the Standard covering TRIs but noted that few firms have implemented them. First mover disadvantage was identified as the primary barrier to achieving this; TPPs are reluctant to invest in TRI capability because they can only realise benefits when all other ecosystem participants implement them too.

It was identified that to maximise the benefits of TRIs, TPPs would be required to provide TRI data and all banks, CMA9 and non-CMA9, should have to use them. While some respondents (primarily TPPs) thought this could be achieved voluntarily via a managed roll-out process which built the confidence needed to overcome the 'chicken and egg' obstacle, most respondents believe that regulatory intervention is required. Other additional measures, such as the development of a "whitelist" of known, low-risk payees were suggested as complementary activities. It was widely acknowledged that a programme of continuous improvement would be needed to ensure the long term-effectiveness of TRIs.

## 1.16. Summary of findings from Ecosystem Strategy Sprints

### 1.16.1. Key Gaps identified

The Ecosystem Sprint highlighted a number of gaps that could constrain the development of open banking going forward. Many of these gaps were highlighted in the Payments and Data Sprint workshops and they were explored further in evidence submissions through the Ecosystem Sprint. The emerging gaps are highlighted below:

#### *1.16.1.1. Gap 1: Development and deployment of an effective fraud prevention strategy*

This was a key concern raised in the payments sprint and further discussed in the ecosystem sprint as it was felt by TPPs to be constraining the development of an open banking ecosystem, in particular for payments.

A range of evidence was provided by TPPs that demonstrated the negative impact on customer journeys of fraud prevention strategies, particularly for high-value payments. Conversion rates varied with the different banks and by transaction size. In addition, further evidence was provided showing customers of certain banks being excluded from certain higher value open banking use cases because of the transaction limits placed on new payees.

In contrast to this, evidence was provided by a few large ASPSPs showing fraud (and attempted fraud) levels in open banking being higher than other digital channels. However, it was clear that a consistent, robust, and detailed breakdown of fraud across open banking was not available, making it difficult to determine appropriate and targeted actions.

Furthermore, the misalignment of incentives and lack of agreed data to be shared between banks and TPPs make voluntary collective action difficult to deliver. Many TPPs believe that account-to-account payments, where the TPP knows the payee, are automatically lower risk than manual bank transfers and deserving of lower friction. Additionally, such friction damages customer perception of their proposition. Whilst ASPSPs have sympathy for this, their evidence is not supportive of the TPPs' belief and their main incentive is to reduce fraud levels, for which they are liable. Customer friction has a much lower impact on their relationship with their customers and, indeed, could be viewed in a positive way.

#### *1.16.1.2. Gap 2: Ensuring a consistent, reliable and resilient open banking ecosystem*

A wide range of other gaps were identified. These have been grouped together as they are potentially constraining the further development of the open banking ecosystem:

**Adoption of and conformance to the UK Open Banking Standard**

Participants from across the ecosystem called for wider and more consistent adoption of the UK Open Banking Standard, both the technical API specifications, the Customer Experience Guidelines, and the operational performance standards. TPPs called for the adoption of the Standard by all UK banks, not just by the large ASPSPs, and some called for more consistency within the Standard, such as making optional data fields mandatory. ASPSPs and expert advisers called for TPPs to adopt the Customer Experience Guidelines.

Clear evidence was presented showing a variance in performance across the ecosystem in API performance, and conversion rates also showed significant variance indicating the opportunity to improve consistency. A trade association provided evidence from a large use-case of open banking

payments showing on average 31% of journeys result in drop off in the ASPSP domain and this varied from 11% to 85% depending on individual ASPSPs.

### Disputes

The issue of disputes was also raised as an area where adoption of a consistent approach may lead to better customer outcomes. However, there was a broad range of views submitted with some participants indicating that the current low level of disputes was evidence that the current operating model was adequate. Other respondents felt that this was an existing vulnerability in the system and the development of A2ART could lead to customer detriment unless a customer dispute and redress mechanism were established. At present customers use debit cards for many retail purchases. This payment mechanism has the added protection of chargebacks where the payer may be able to recover their money if something goes wrong with the purchase, such as goods or services are not delivered. Open banking payments are sometimes thought to be like paying with cash as they do not include a mechanism like chargebacks. Some respondents felt that where open banking payments substitute for card payments customers may be exposed to this “purchase risk” but other respondents felt that existing mechanisms such as the Consumer Rights Act provide adequate protection for purchase risk.

### Customer understanding, awareness, and trust in open banking

The Committee specifically asked about awareness and trust, and responses to these questions highlighted diverse opinions across the ecosystem as to whether this was an area of concern or not, and what to do about it. Contradictory evidence was submitted as to whether there was a trust gap or not, with some respondents suggesting that the enhancement of customer experience of using open banking-enabled services and the value of the propositions were more important ways to build customer confidence. There was also a broad range of views as to whether a trust mark was needed and whether it should be for payments, for data or for both.

### Transparency of Consent

Whilst this is a subset of customer understanding there were a number of responses that highlighted an opportunity to improve the transparency of consent, either by evolving the existing dashboards or more radically by making consent details available via API to enable providers to build ecosystem-wide dashboards.

### Onward Sharing of Data

There is a broad range of views from respondents as to whether onward sharing of customer data by a TPP is a material risk to the development of open banking. Three schools of thought emerged from the responses:

- There is no evidence of significant issues in this space. Existing regulation provides sufficient checks and balances, and onward sharing is beneficial to the development of the ecosystem. It should be allowed to continue as today.

- Onward sharing is not always clear to consumers and small businesses today and we should evolve guidance and control tools to make it more visible.

- Onward sharing is a significant risk to consumers, and we should evolve regulation to control onward sharing more tightly, limit it or stop it altogether data.

#### Crisis Management

Most respondents felt that central crisis management planning was not necessary for the functionally more distributed network that is open banking and would represent duplication of effort. However, some respondents felt that the centralisation of trust services did represent a risk to the industry and the creation of a crisis management plan for this key infrastructure may be beneficial.

### *1.16.1.3. Gap 3: Restrictions to the expansion of open banking*

A number of respondents referenced the Committee's policy objective of the expansion of open banking. During the sprint discussion meetings there was an emerging view, especially from TPPs, that regulatory intervention would be required for the expansion of open banking due to the misalignment of incentives across the ecosystem. There were two areas identified for potential expansion:

#### Expansion of VRPs for Non-sweeping use cases

A number of TPP responses felt that access to VRPs for non-sweeping use cases was an important enabler for the ongoing development of open banking payments. Two key constraints to this were identified:

- **Customer Protection:** large ASPSPs, expert advisers, trade associations and TPPs highlighted that a clear and well-understood customer protection and liability regime was required for the expansion of VRPs. However, there were very different views as to the nature of the regime, where liability would reside, and the level of purchase protection offered to end users.
- **Inter-firm Pricing Arrangements:** The pricing of non-sweeping VRPs from banks to TPPs was another area where there was striking divergence across the respondents. On the one hand, there were advocates for letting the market determine the price for access. Others felt that this would not enable the market to develop as banks would set the price at a level that prevented the cannibalisation of card revenues, and therefore that a regulatory price cap may be the right way to support market development. However, other respondents expressed a view that charging for initiation of VRPs would undermine the viability of VRPs as an effective payment mechanism and so access for all payment initiation services, including VRPs for non-sweeping, should remain free.

#### Expansion of open banking data sharing to open finance

There was a common view that regulation would be required to open up new products, such as savings, mortgages or lending products, for open banking data sharing. Experience from overseas markets reinforced this opinion with the expansion of open banking data sharing in the US, where there is no regulatory obligation, being very slow with high barriers to entry in comparison with Australia, where a clear regulatory framework is accelerating data sharing, for instance, including the opening up of transportation and utility data sets.

### 1.16.2. Potential Prioritised Initiatives

The evidence in the ecosystem sprint identified a wide range of potential priority areas including issues raised in the Payments and Data Sprints, such as the expansion of VRPs, ensuring there is a robust and well understood purchase protection regime in place, and enabling access to new data sets. The evidence on these topics supported the priorities discussed in the Payments and Data Sprints and so will not be duplicated here.

The overarching theme from the Ecosystem Sprint was an emerging priority from the ecosystem respondents to ensure that open banking has robust foundations both in the ongoing operational performance of the ecosystem (System & Standards) and regarding the oversight and conformance of the system.

#### *1.16.2.1. Ways to deliver a robust and vibrant ecosystem*

Ensuring that open banking operates as a robust and reliable service was a key theme in all the sprints and the Ecosystem Sprint explored how this might be achieved. It was felt that a focus on standardisation would be an important priority in delivering a robust and vibrant ecosystem and there were a number of elements to achieve this:

**Enhancement of the Standard**

A number of respondents felt that removing some of the optionality within the Standard would ensure that consistent information would flow from ASPSP to TPP irrespective of which firm was involved. At present not all banks fill optional data fields. Some banks felt the reduction of optionality was also important on the TPP side with TPPs being required to provide the information in the TRI fields, where applicable. Some ASPSPs recommended caution with any expansion of the Standard, referencing the under-utilised functionalities delivered already as part of the CMA Order. They felt that new propositions and markets needed to be tested to provide the evidence of user demand.

**Whole of market conformance**

There was a common view across many, typically TPP respondents, that the level of oversight currently in place for the CMA9 should be extended to all ASPSP participants to create a whole of market conformance regime.

Some evidence suggested that it would be helpful for TPPs to also be subject to a specific conformance regime. This could cover:

- Implementation of and conformance to TRIs required by ASPSPs.
- Provision of transparency and control to consumers, including consent dashboards, and visibility of onward sharing.
- Agreement to follow guidance on VRPs for sweeping.

**MLAs**

There was limited detail and no consensus on how the initiatives to achieve standardisation referenced above could be achieved. MLAs were often cited as a way to achieve these objectives as well as others such as expansion of VRPs, development of customer protection and the expansion of data sharing. An MLA would provide a contractual basis to encourage participants to adhere to agreed rules, but again there was a limited amount of detail on how that can be achieved. Some

respondents suggested that the development of MLAs should be left to the market, arguing that they were a natural progression from commercial bilateral agreements. A number of expert advisers and TPPs, as well as an ASPSP, expressed concerns that bilateral agreements had the potential to distort and fragment the market. Their view was that a market-driven proliferation of bilateral agreements is likely to lead to a less efficient market that fails to exert the desired competitive pressures on card payments, and to market fragmentation which will cause customer confusion (or possible harm), eroding long term confidence in open banking.

A widely held view was that some form of regulatory intervention would be required for the development of MLAs but there was no consensus on the nature or scope of the intervention, as it would be difficult to agree on a commercial basis upon which to align incentives. Regulatory intervention was deemed particularly important for access and several respondents felt that price and customer protection should also have regulatory backing. Many TPPs recommended a mixed approach with regulatory intervention in specific areas, but also enabling the market to find solutions in less contentious areas, for example agreeing to a process to manage disputes.

#### *1.16.2.2. Vision for Open Banking*

When determining the best way for the ecosystem to develop, several large ASPSPs and some trade associations felt that it would not be possible to determine the best structure(s) to manage the developing ecosystem until there was clarity around the vision for open banking and open finance and the outcomes that the regulatory authorities wanted to achieve.

Across the respondents there was also a very broad range of ambition for open banking, with banks typically being more cautious and TPPs more expansive in their ambition. This was not universal, however, with one bank in the ecosystem strategy sprint discussion meeting promoting a very expansive vision for open finance.

#### *1.16.2.3. Role of the Future Entity and its funding*

Respondents identified a range of services required for the safe and sustainable operation of open banking:

a. **Maintenance and development of the Standards**
b. **Monitoring and ensuring conformance to the Standards**
c. **Provision of digital certificates (Directory - certificates)**
d. **Permission checking (Directory - permissions)**
e. **Service support (e.g., help desk and issue escalation).**

However, there were divergent views around which entity should provide individual services. At present the OBIE undertakes these activities but there were differing views around which of these activities should form part of the remit of any Future Entity.

**Maintenance and development of the Standards**

Most respondents recommended that the Future Entity should be responsible for the maintenance and development of the standard. There were no dissenting voices, although one trade association felt closer harmonisation with European regulation would be beneficial. Beyond maintaining and developing the standard there were divergent views regarding the remit of the Future Entity. One

large ASPSP suggested that the Future Entity should become a centre of excellence for all smart data standards which would ensure all smart data initiatives are as aligned as possible.

### Monitoring and ensuring conformance to the Standards

Most respondents indicated that they expected the Future Entity to be involved in ensuring conformance, but the nature of the envisaged role varied. For some it was around evidence collection to enable the appropriate regulator to act, but others recommended that the Future Entity should be given enforcement powers to require participants either to provide data or even to compel participants to undertake corrective action when performance falls short of expectations.

### Other Activities

Beyond these activities there were more wide-ranging views regarding which activities needed to be supported by the Future Entity and which could be delivered by others. A platform summarised the view of many respondents when it suggested that the Future Entity should only step into issues where industry cannot provide a solution. The provision of Directory Services, both certificates and the permission checking service, was an area where many banks and a number of other respondents felt that market-driven solutions might provide a more resilient and cost-effective solution. TPPs were not averse to this change but cautioned that any change may risk disruption to the market and any potential disruption had to be carefully managed.

Limited evidence was provided around other support services such as a help desk, or provision of a centralised dispute management service (if required).

### Funding

Many participants provided viewpoints on the funding of the Future Entity, which was a key priority for resolution. However, there was a range of divergent views on this topic. There was widespread support for the notion of a fair and equitable funding model, but no consensus on the details of how to bring that about.

A few respondents felt that some of the Standards development, maintenance and conformance monitoring ("Core Services") currently undertaken by the OBIE should form the basis of a capability to underpin open finance and the broader Smart Data Initiative. The potential economic prosperity brought about by digitisation and the expansion of fintech from open finance and Smart Data suggested to some respondents that there was a strong case for this central core to be, initially, publicly funded.

Other respondents made the case for some form of regulatory levy to pay for Core Services. Expert advisers suggested that a levy provided a means to separate the funding of an institution from its governance to ensure that the largest funders would not have undue influence.

There were more divergent views around the funding of other activities, such as the Directory, with some respondents citing that these services can be provided by the market, as they are in Europe and so would not require any central funding.

The most common response to funding was that participants should fund the central services, and this could be done by some form of tiered membership structure (e.g., based on turnover or market size) or a pay by usage model (e.g., based on API calls or transactions) or a mix of both depending on the services. Some respondents cautioned against a usage-based funding model, since it may disincentivise certain use cases such as propositions aiming to support vulnerable customers.

# EVIDENCE AND FINDINGS FROM THE FIRST ROUND OF STRATEGY SPRINTS

## 1.17. First Payments Strategy Sprint

### 1.17.1. Question 1: Resolving Barriers

***What should the approach be to resolve issues and possible barriers around open banking payments, for example better supporting high-value payments? Should a risk-based approach to open banking payments be considered or not? Please provide rationale and evidence. How can account providers and TPPs work together to manage the associated risks (if any)? Are there particular use-cases and/or scenarios in which additional or different models are required or not? Please provide rationale and evidence.***

#### *1.17.1.1. Introduction*

For most TPPs, some large ASPSPs and expert advisers, this question acted as a "catch-all" for all the issues, concerns and even potential remedies held by different stakeholders. We have tried to keep the summary to this question to issues and barriers with a particular focus on high-value payments and risk-based approaches. Other issues, such as functional capabilities, are covered extensively in other questions.

#### *1.17.1.2. Areas of Discussion*

**Area of Discussion 1: Payment Limits**

There was a general consensus amongst TPPs that banks' application of their own online banking payment limits to open banking transactions made some propositions unviable. Most TPPs counted this as their number one barrier, although some added the proviso that this is an immediate issue, that needed to be urgently addressed. In addition, there were broader concerns around appropriate risk management and messaging by ASPSPs to prevent push payment scams.

From an ASPSPs' perspective, higher value payments are considered to be more prone to fraud but there was limited quantitative evidence provided. Open banking payments are typically of high-value compared to cards: one large ASPSP stated that the average open banking payment value is £450 compared to less than £50 for cards, pointing out that, whilst high-value payments represent an opportunity for PISPs, they represent risks for banks.

TPPs put forward evidence of bank payment limits ranging from £2,000 to £10,000 and stating that this meant that many use-cases were not viable as a result. Whilst banks argued that this replicated limits in their own channels, some TPPs expressed the view that some banks were not adhering to FCA guidance on this issue which stated that the open banking payment limit must be equivalent to the highest across all of their channels (e.g., the higher of in-app and web browser).

All stakeholders that commented on this issue accepted that there was scope for improvement, based both on enhanced (and many respondents suggested standardised) data sharing between participants (primarily between PISP and sending bank), and changes to liability arrangements.

There were some differences within this broad consensus, however. One large ASPSP felt that PISPs should be required to sign up to Confirmation of Payee (CoP) and the Contingent Reimbursement Model (CRM) Code, while one TPP made the case that the bank receiving the payment should be liable for APP fraud as they undertake due diligence on the payee. However, most TPPs accepted that a model whereby they would take on some or all liability if they had undertaken due diligence (KYC) on the payee would be beneficial, an arrangement supported by the large ASPSPs.

In addition, there were several additional nuances to this issue:

- Many stakeholders supported a level of standardisation (and, suggested by one large ASPSP and some TPPs, backed by a regulatory requirement) of TRIs, i.e., sharing of data and attributes by the PISP to the sending bank.
- Whilst some TPPs argued that APP fraud should be minimal since they would having have undertaken KYC on the payee, others accepted that there were some use-cases where this would not be the case (such as peer-to-peer payments).
- Two large ASPSPs stated that fraud levels were higher for open banking payments than for standard inter-bank transfers. The empirical evidence provided was inconclusive on this point, with different definitions used (such as attempted fraud versus actual fraud), and one TPP stating that there were only two instances of open banking payments fraud reported to the FCA (although it was not clear whether this only included unauthorised rather than authorised payment fraud). There was a consensus that better data would be helpful.
- Some TPPs felt that consistency of limits and treatment across the ecosystem would help consumers, whereas a large ASPSP highlighted in the discussion that standardised limits could be detrimental as limits might be linked to an individual's circumstances and risk appetite.
- Some actors in the ecosystem suggested that risk management was subsidiary to a wider issue of commercial arrangements amongst participants in the ecosystem.

### Area of Discussion 2: Misalignment or lack of commercial incentives

Whilst articulating the issue in different ways, large ASPSPs, expert advisers and TPPs were concerned with a lack of overall business case, a misalignment of incentives and/or end user (payee or merchant) costs. This led many stakeholders to express scepticism about the widespread extension of open banking payments to the full range of use-cases, especially A2ARTs. Specifically:

- Three large ASPSPs questioned whether there was a business case for further investment in open banking payments at all.
- For non-sweeping VRPs, one large TPP stated that it was not confident there was an economic arrangement that could compensate banks for lost card revenue (interchange and scheme rebates) while delivering savings for merchants. Several TPPs mentioned that in bilateral contract discussions, some banks were asking for fees higher than current debit card interchange fees, meaning that the business case to merchants would not stand up.
- One payment platform and three TPPs referenced the costs of inbound Faster Payments, which a group of TPPs suggested were over twice the cost of the SEPA (eurozone) payment system, meaning that merchant bank prices could make low-value payments using open banking uneconomic to accept compared with cards. (It is to be noted that card fees are a percentage of the value of the transaction whereas Faster Payments are priced at a fixed

fee per transaction). Some TPPs also commented that this problem would be exacerbated if the significant investment cost of the NPA was to be passed on.
- It was also noted that the current liability model, in particular for APP fraud, creates misaligned incentives (see above for more detail).
- One independent expert and a trade association commented that the existence of debit card interchange coupled with the no-surcharging rule in the PSRs meant that there was no case for ASPSPs to invest in ACH-based payment types as competitors to cards. This was because ASPSPs see debit cards as an income stream, whereas open banking payments would generate a Faster Payments cost.

This generally negative viewpoint was not shared by all. Several ASPSPs and one TPP referenced the low level of market maturity of open banking payments, accepting that it takes time for markets to stabilise, mature and innovate. A number of ASPSPs commented on the success of HMRC in taking open banking payments, and a TPP also made the case for open banking payments competing not with cards but with inter-bank transfers, where there were substantial benefits to both payers and payees (and without the disincentives).

### Area of Discussion 3: Customer experience

All TPPs referenced poor or inconsistent customer experiences – of some form or other – as a barrier to open banking payments usage. One TPP suggested that it was the key barrier, stating: "*We believe that the lack of adoption is simply due to poor user experiences and functional limitations, which are not on par with established payment options — such as cards and alternative payment methods by e-money institutions. Although the existence of strong customer authentication (SCA) does not present an obstacle per se, we believe that the current design of the SCA journeys by many of the UK banks simply do not allow payment initiation service providers (PISPs) to offer a more compelling payment experience than established solutions*."

A range of specific issues underneath the general topic of customer experience were raised:

- **Low conversion rates** (i.e., the ratio of completed payment journeys compared with those that were started). Whilst one TPP stated that they were broadly content with their conversion rate of 84%, another stated that often poorly documented and frequent downtime / maintenance windows substantially affected such conversion rates, giving the example of one bank having 13 downtime events over 12 days, when payment conversion rates dropped from 52% to 8%. Additional consideration of these topics is included in Question 6 (Access and Reliability).
- **Excessive authentication protocols**, including one bank that, according to a TPP, required a phone call to set up a new payee (this could take up to an hour). One platform and several TPPs suggested that an alternative **"delegated" or "open" authentication** would improve comparisons with card-based authentication. This network also suggested that VRPs could provide a solution. Another platform representative also commented on the clunkiness of open banking payment journeys.
- **Extra screens and additional messaging.** As one TPP stated, "We believe that the lack of adoption is simply due to poor user experiences and functional limitations, which are not on par with established payment options."
- **Lack of granularity and consistency** in providing TPPs with **error codes**, so there was a lack of understanding of what went wrong.

- Sometimes there was **no redirection back** to the TPP when something went wrong (referenced by an ASPSP).
- **Dashboards** showing details of VRPs difficult to find. Some TPPs suggested they were in the wrong place, preferring placement alongside regular payments rather than with other consents.
- Delay in executing the payment, or decline.
- Lack of use of SCA exemptions such as low-value exemption of £25.

A number of these ideas are discussed in more detail in the section on Question 4 (Functional Capabilities). Additionally, a number of respondents considered issues of down-time and low conversion rates in their responses on Q6 (Access and Reliability).

### Area of Discussion 4: Unnecessary regulatory interventions

One ASPSP suggested that the CMA Order, and its interpretation, imposed a barrier by narrowing the industry's focus and diverting resources away from market-led innovations beyond the Order. In its opinion, the Order led to wasted development costs on certain functionality which had no market demand, for example: International Payments, Bulk/File Payments and two-way notice of revocation.

### Area of Discussion 5: Lack of API functionality

This is covered in more detail in Question 4 (Functional Capabilities). However, one of the most significant blockers from a functionality point of view was improvements to payments certainty, for example by earmarking of funds or providing the equivalent of an authorisation (i.e., guaranteed settlement). This was of particular importance to those use-cases where certainty was needed while the customer was in-session online.

### Area of Discussion 6: Variable Recurring Payments for Sweeping

Whilst VRPs for non-sweeping use cases are mentioned extensively in response to other questions, two TPPs stated that they believed the definition of "sweeping" was both overly complex and restrictive, thereby presenting a barrier to adoption.

### Area of Discussion 7: Lack of clarity around consumer protection including purchase risk

One independent expert stated that a clear and comprehensive fraud liability and dispute resolution framework was required, to be overseen by an independent regulator. Whilst there was consensus amongst TPPs not to overlay card-based protections such as chargeback systems onto open banking payments, some ASPSPs were looking for at least equivalent protections to those provided with cards. One ASPSP went further and stated that consumer protection needed to "at least equal the processes provided within the cards schemes to be a viable substitute".

More detail is provided in Question 5 (Dispute Processes).

#### *1.17.1.3. Potential Areas of Alignment*

Responses in this area were wide-ranging. As such, it is hard to definitively identify areas of alignment. As indicated, there is additional detail provided in the evidence summarised in other sections.

There was a significant volume of data and challenging opinions expressed in the area of high-value payments, however we consider that some emerging areas of alignment can be considered:

- There is common ground that fraud prevention is vitally important and some form of resolution is required in this space, even if there is not agreement on the appropriate methods. The issues experienced in relation to high-value transactions are a particular challenge highlighted by respondents of all types, although ASPSPs tend to consider this issue through the lens of fraud management and TPPs through the lens of payment completion and certainty.
- It is also clear that this is a priority for many in the ecosystem, notwithstanding the distinction drawn above.
- Finally, there is broad agreement that a territory to be explored to improve this situation is likely to lie in the more effective sharing of data between TPPs and ASPSPs.

Beyond these broad areas of alignment however views and other proposed solutions to bridge this gap are varied and at times contradictory and additional work will be required by the Committee to consider how to take forward work in this area. There is additional detail on many of the areas highlighted in this section in responses to other questions, including:

- Misaligned commercial structures: MLAs (Section 4.3)
- Functional Enhancements: Functional Capabilities (Section 4.4)

### 1.17.2. Question 2: Promoting Adoption

***What is needed to promote the adoption of open banking account-to-account transactions, including recommendations and requirements from end-users and merchants? Please provide rationale and evidence.***

#### *1.17.2.1. Areas of Discussion*

**Area of Discussion 1: Consistency and reliability**

A wide range of views was expressed across the submissions although a common theme from all participant groups was the need for consistency and reliability. This theme was repeated across a number of answers by ASPSPs, TPPs and expert advisers. Fifteen respondents felt that consistency in user experience and end-to-end reliability was key to promoting adoption. A number of ASPSPs and TPPs felt that adherence to the open banking standard (for all ASPSPs and TPPs) and more consistency and standardisation across error messaging and responses would help with adoption.

**Area of Discussion 2: Purchase Protection**

This was cited as vital for promotion of open banking payments and a common topic across a number of answers. This was supported by expert advisers, ASPSPs and TPPs and platforms. However, there were limited details around what a customer protection regime might look like. There was a common view that customers need to understand the regime but a range of views around the broad scope of a protection regime. Some respondents suggested a similar model to cards. However, other respondents warned that replicating cards' consumer protection regime would not be an optimal outcome, as this adds costs and leaves no room for differentiation between cards and open banking. Expert advisers and a bank warned against competing on purchase protection as it could result in a race to the bottom in which protections are given up in return for cheaper payments, ultimately harming consumers and undermining adoption. They believe that parity in protections between payment rails is best achieved via a centrally set standard minimum standard for all payment methods.

This is discussed in more detail in Question 5 (Dispute Processes)

**Area of Discussion 3: Variable Recurring Payments (VRPs)**

In response to this question, and more generally across responses, most TPPs recommended that mandating VRPs for all transactions, not just sweeping, would be key to the future development of the market for open banking payments. This view was not shared by ASPSPs who were largely silent on the matter in these responses.

**Area of Discussion 4: Incentives.**

Many respondents referenced ensuring that there were appropriate incentives for all parties being key to the promotion of open banking payments, but there was no consensus around the approach to be taken. Representatives of retailers and one independent expert suggested that abolition of interchange on debit cards was a way to remove the incentives for promoting debit card use above open banking payments. Other firms, including ASPSPs, TPPs and platforms recommended that there need to be viable commercial incentives for all parties. However, from the responses and the Sprint discussion it was noted that this might not be possible. ASPSPs generally expressed the need to be appropriately compensated for the costs of initiating open banking payments. Several TPPs cited that the costs of open banking payments need to be such that they are more cost competitive than cards for merchants, with several noting that the cost of receiving a Faster Payment can make open

banking payments less cost-effective than cards, particularly for lower value payments. A number of respondents felt that interventions needed to be regulatory in nature and that initiation of VRPs should be mandated at no cost to TPPs, although other TPPs felt that some commercial model may be required for VRPs.

**Area of Discussion 5: Trust mark**

The question of trust marks prompted a wide range of viewpoints in evidence. Across the ecosystem respondents, when they commented on the matter, felt that common language and terminology were required. Several TPPs referenced what they believed to be unnecessary warnings from certain ASPSPs that in their view undermined trust in open banking. However, across the TPP community there was some disagreement on trust marks, with some respondents feeling that a trust mark would be beneficial whereas others felt it would be anti-competitive. One ASPSP and some TPPs referenced previous work by OBIE suggesting that trust marks do not add much value, whereas some platforms felt that lack of a brand would impact the take-up of open banking payments. The issue of trust marks is also discussed and there is additional detail in the Ecosystem Sprint, Question 7.

**Area of Discussion 6: Payment Certainty**

Certainty of the fate of an open banking payment was commonly cited by many TPPs as vital to drive adoption by merchants. This topic was also referenced in the Sprint Discussion meeting, where it was clarified that the certainty of fate of a payment once it reaches the Faster Payments network is well known. The issue in question here is whether the PISP, or the merchant via the PISP, can access this information in a timely manner to support different propositions. Certainty of fate was not mentioned as an issue by ASPSPs. This is discussed in more detail in the responses to Question 4 (Functional Capabilities).

**Area of Discussion 7: Demand Factors.**

Two ASPSPs questioned the need for promotion of open banking as they regard the open banking payment market as well-established and growing. Incentivising customers to move from cards as a payment method was highlighted as a challenge as the cards market was felt to be functioning well for consumers.

#### *1.17.2.2. Potential Areas of Alignment*

In response to this question, there was potential alignment around the need to drive greater consistency and reliability, as a driver of additional adoption. As is to be expected with an open question of this type, respondents put forward a wide variety of other priorities to drive adoption, with some being proposed by a number of respondents, but no other area emerged as a consistent theme or priority across the ecosystem.

In particular discussions on consumer protection, incentives and trust marks exhibited wide divergence in responses, a number of which are picked up in other sections.

Two responses from ASPSPs went further and suggested that the market is already progressing and growing and therefore suggested that limited intervention was required.

### 1.17.3. Question 3: Multilateral Agreements

***What areas would MLAs covering services beyond the Order and existing regulations need to cover in order to facilitate continued development of open banking payments in a safe and efficient manner? Please provide rationale and evidence.***

#### *1.17.3.1. Areas of Discussion*

Note that responses there are evidence summaries related to MLAs in the Payments Sprint (here), the Data Sprint (Section 5.8) and the Ecosystem Sprint (Section 6.3).

**Area of Discussion 1: Should multilateral contracts be voluntary or mandatory?**

Whilst there was general support for some form of MLAs there was no consensus as to how this could be brought about. The breadth of responses ranged from having regulatory driven or approved agreements through to entirely leaving the market to solve these. Some respondents felt a mixture of the two different approaches was appropriate, with regulatory obligations for access to open banking APIs (including VRPs) and / or regulatory intervention on price varies by respondents (e.g., a cap on fees / setting an appropriate fee level / ensure there is no fee).

Two expert advisers expressed concerns that lack of regulatory oversight could lead to an undermining of consumer protections.

Some interesting quotes on this topic were:

*"Ultimately the market will need to assess and consider the options at play."* – ASPSP

*"Our preference is that we participate in a regulatory approved [MLA] … we believe the PSR plays an important role in ensuring that access to such arrangements is open."* – TPP

*"Our preference would be for the regulator(s) to establish a scheme for open banking payments."* – independent expert

**Area of Discussion 2: What should the scope be for multilateral contracts?**

There was a divergent view on the depth of an MLA, with some suggesting that it would need to be the equivalent of an open banking payments **scheme**, whilst others felt that a **framework** agreement would suffice. A number of respondents suggested that any agreement needed to have appropriate levels of compulsion to participate and confirm to the rules.

One TPP proposed that any agreement should be constructed as a Payment Arrangement. This would ensure regulatory oversight by the Payment Systems Regulator.

**Area of Discussion 3: What is the right approach on pricing and cost?**

Some TPPs cited the need for free access to VRP APIs whereas others recognised the need for ASPSPs to be compensated for access to non-sweeping VRPs, but this needed to be cheaper than the cost of cards.

Many ASPSPs also referenced the need for any MLAs to be able to support them making a commercial return for activities undertaken. More comments on pricing and cost can be found in the responses to Question 7.

#### *1.17.3.2. Potential Areas of Alignment*

Whilst there was no consensus for the adoption of MLAs there was broad support from ASPSPs, TPPs and platforms that multilateral contracts would be most beneficial to cover disputes and customer protection and helping to ensure there is consistency in where responsibility lies when things go wrong. However, there was limited definition of exactly what should be covered under each heading.

When referenced, respondents generally preferred MLAs to bilateral agreements, with a number of TPPs and expert advisers citing that bilateral agreements were at risk of disadvantaging smaller players who may not have the resources to negotiate them with all ASPSPs. It was also noted that any negotiation may not be balanced as large ASPSPs have a natural monopoly of access to their customers.

### 1.17.4. Question 4: Functional Capabilities

***Functional capability: what are the most appropriate use cases to consider, and what additional functional capabilities and considerations (e.g., risk management) would be needed to support them? Please provide rationale and evidence.***

#### *1.17.4.1. Areas of Discussion*

**Area of Discussion 1: Most appropriate use cases**

Across the 34 submissions received there was a broad consensus around the priority use cases for open banking payments, with most agreeing that e-commerce payments should be the highest priority use case.

Beyond this top priority use case, there were a wide range of use cases cited by respondents, including:

- Bill payment
- Recurring payments
- Face-to-face retail
- Transactions where the final amount is not fixed at point of initiation (e.g., grocery, automated fuel)
- SME payments.

However, a minority of respondents (three), suggested that thinking in terms of use cases was too restrictive and encouraged the Committee to think of open banking as an enabling platform for open finance and other data sharing opportunities.

One response identified a unique set of use cases which are worth highlighting given their importance in supporting marginalised or vulnerable consumers. One TPP response focused on the ability for open banking payments to evolve into a solution which could provide cash withdrawal and cash deposit services.

Given the regulatory focus on access to cash, the Committee may wish to consider this proposal further. This response also suggested a potential solution to the challenge that only digitally active consumers can use open banking, suggesting that the Standard could be evolved so that customers could use their payment card to identify themselves, thereby enabling participation by a much broader cross section of the UK population. The submission argued strongly that access to cash withdrawal and deposits was of critical importance for many UK citizens and that open banking could play a key role in broadening access to both these functions. We note that an ASPSP submission highlighted that only 60% of its customers were digitally enabled.

**Area of Discussion 2: Additional capabilities and considerations**

In total, nine broad additional capabilities and considerations were identified by respondents, with some areas obtaining widespread support and others featuring in only a minority of responses.

First, we list these nine areas, ranked by the number of respondents who cited them, and including some observations in terms of the types of entity requesting that the Committee consider the development of these capabilities and considerations.

**1. Greater certainty and clarity on payment outcome:** there are a number of overlapping submissions in this area, including:

- Calls for **more granular and meaningful status messages**. One TPP submission set out the rationale as follows: "Surely, the industry would benefit [from] ... enhanced information reporting requirements on the payment status, which would allow the PISP to give the merchants confidence that they will receive the transaction amount. However, there are ways to innovate around such deficits and such information can be offered by ASPSPs on commercial terms." One payment platform provided evidence on status messages that showed that only, "19.4% of payments initiated resulted in a payment status confirming certainty of fate".
- New functionality enabling PISPs to **ear-mark funds** similar to a card authorisation. An example submission from an ASPSP suggested that *"there should be a guaranteed payment / settlement scheme developed to allow merchant confidence in accepting the payment. This may align with the proposals in the ongoing SEPA SPAA work[6]."*
- A new type of payment which is either **executed immediately or declined**. As an example, a TPP commented as follows: "… the only other functional capability we can see value in that is not available today from open banking or the underlying Faster Payments system is a pay 'now or never' capability. This capability would support payments where the receiving business needs certainty in real time that either a payment has been made or hasn't."

Functional enhancements in this area were very widely cited in written evidence. Participants proposing developments in this area included two ASPSPs, alongside nine TPPs. Additionally, two platforms identified this as a priority area as did both expert advisers. We must note one dissenting voice from the TPP community who stated that, "*payment certainty is not a major issue*" in their experience.

It is also worth highlighting that there appeared to be differences between the written evidence and the points raised in the discussion session on 23 September 2022. In that session, three TPPs questioned whether there was a functional gap in relation to payment certainty.

Also, important to highlight is that two ASPSP responses identified no additional functional capabilities or considerations required beyond items covered elsewhere in their submission.

Given the views expressed in these two ASPSP submissions, which identified no additional functionality or capability required to support open banking payments, and some TPP views in writing and at the discussion session, this area does not have unanimous backing as a priority for functional enhancement. In part this can be explained by the fact that there are three overlapping functional enhancements in this area: status messages, ear-marking and a 'now or never' functionality. All three of these enhancements can be considered under the broad umbrella of payment certainty, however, in technical terms they are very different.

We suggest therefore that this is as an area of emergent agreement, but with the following important caveats:

- One TPP explicitly stated it wasn't a priority for them.
- Two ASPSPs did not propose any technical enhancements.

[6] SPAA refers to the SEPA Payment Account Access proposed scheme.

- The discussion session highlighted further differences of opinion on this area, the appropriate technical solution to the challenge and its prioritisation.

**2. Expansion of VRPs:** a number of submissions called on the Committee to expand the mandatory or free provision of VRPs functionality beyond sweeping use cases. Some wanted it to be available in all use cases, some called for a more measured expansion, some accepted that commercial fees would be required, others called for it be provided without cost. Expansion of VRPs beyond sweeping was therefore a common request, although the precise mechanics for this expansion saw quite wide variance.

ASPSPs did not support the mandatory expansion of VRPs but some considered it to be a commercial opportunity. It was predominantly TPPs and retailers who called for this.

**3. Error Code Enhancements:** many participants highlighted challenges in understanding the outcome of a payment initiation, when unsuccessful. Many participants were not able to accurately determine the reason for payment failure and were therefore unable to advise their customers or take appropriate action. As one TPP described in their submission: "*Currently, many of the bank APIs provide generic error and fail messages which makes it impossible for PISPs to correctly handle customers. Providing detailed status through the flow as well as error codes would allow the PISP to inform the customer of what they can do to complete the payment."*

This functionality was highlighted by some TPPs and Other Banks (who also operate as TPPs).

**4. Delegated or Open Authentication:** some participants suggested that PISPs should be allowed, in certain circumstances, to undertake SCA. This flexibility would enable more seamless, friction-free payment experiences, particularly in low-value scenarios for example. The independent expert also proposed that Regulators require that global technology companies open up access to the secure element and NFC capability on smart phones to expand usage and remove friction associated with open banking payments.

This was highlighted by some TPPs and three platforms.

**5. Improve data flow from ASPSP to PISP:** some participants identified a need for additional data to be shared from ASPSP to PISP, either to help with KYC or to identify fraud. In some cases, the need was for this data to be provided prior to payment initiation. Dataflow from PISP to ASPSP is extensively considered in the responses to Question 1 (Resolving Barriers).

This was highlighted by some TPPs and one platform.

**6. Ability to Change Final Settlement Figure:** a key gap identified by some participants was that open banking payments are initiated with a fixed amount. In use cases like grocery, hotels and automated fuel dispensers this is not viable. These participants called for a solution that allowed the final amount to be adjusted (within tolerance) once the final transaction figure was known.

This was mentioned by an ASPSP, a TPP and one platform.

**7. Actor visibility and payment references:** some participants highlighted the importance that the payer has good quality, accurate information about who they are paying, which works across different payment configurations. The Open Banking Standard today has a solution to this which uses software statements. This was described by a TPP submission as *"an unnecessary and unscalable requirement that would make operational deployment of VRP services massively complex for TPPs and ASPSPs*".

This was mentioned by an ASPSP, two TPPs, a consumer expert and a platform. See also Section 5.2, Discussion Area 3 where there is a broader discussion of clarity of permissions. Whilst this related to the Data Sprint, it also has relevance for the Payments Sprint.

**8**. **SME payments:** some respondents highlighted the importance of enhancing particular aspects of SME-specific payments, including how batch payments work and multi-authentication flows.

This was mentioned by two TPP submissions.

**9. Consistent Guidelines for Face-to-Face payments:** some respondents called on the Committee to ensure that additional guidance was provided to ensure consistent implementations in Face-to-Face environments (such as QR codes).

This was mentioned by one ASPSP and a platform.

**10. Other Proposals**

In addition, the following proposals were submitted by just one respondent:

- Combined consents covering payments and data in one journey.
- Introduce cards as an alternative means of identity to authenticate customers without digital access and allow them to make payments.
- A reverse consent journey to enable deposits.
- The provision of balance in journeys to support customer control.
- The ability for open banking payments to use contactless functionality in smartphones
- Enhancements to the Standing Order standard implementation, which in its current form has a number of issues preventing its use by TPPs.

### *1.17.4.2. Emerging Areas of Agreement*

On reviewing the submissions, it is fair to conclude that there are two potential areas of alignment:

Firstly, not all participants specified particular use cases, but across the responses, e-commerce was most cited as the priority, followed by bill payment and recurring payments.

Secondly, with caveats, it is also reasonable to conclude that work is required to consider ways to provide PISPs, merchants and consumers greater certainty at point of making the payment and following payment submission. It is important to highlight that verbal evidence was more nuanced on this topic and that there are a number of diverse options to provide payment certainty.

Beyond these two areas of potential alignment, however, there was significant scope for respondents to interpret the question in different ways and a multiplicity of responses is to be expected.

The Committee may therefore need to consider the following areas which showed a significant lack of alignment:

- From responses, it is unclear which of the many proposed areas of additional functionality should be progressed for further examination and consideration. There is a long list, each with passionate and evidence-based responses supporting each area of functionality.
- It is notable that a few ASPSPs (although not all), did not identify any new functional capabilities that were required. This is in stark contrast to many TPP responses which identified a long list of potential areas of development.
- The expansion of VRPs was one of the most frequently cited developments by TPPs and retailers. It was not proposed by a single ASPSP, suggesting that the development and evolution of this type of payment is likely to cause significant divergence.

### 1.17.5. Question 5: Dispute Processes

***Dispute process: how should payment disputes be managed, and what does this imply for consumer protection and redress? Please provide rationale and evidence.***

#### *1.17.5.1. Areas of Discussion*

Note that disputes are also considered in Section 6.4 of the Ecosystem Sprint.

**Area of Discussion 1: Types of disputes**

Evidence from some respondents encouraged greater clarity on different types of disputes. A TPP drew the distinction between:

- Payment disputes: issues related to the execution of a payment, errors, payment not authorised, etc.
- Purchase disputes: situations where goods or services not received or not as described, or the firm goes out of business before being able to deliver a good or service.

Whilst this feedback was only provided by a small number of respondents, we consider it a helpful distinction to draw to provide more helpful feedback to the Committee when considering the management of dispute processes and we have adopted it in this section.

**Area of Discussion 2: Managing disputes**

Within the evidence there was some agreement that the following elements would be helpful to support the development of the open banking payments ecosystem and the way that payment disputes are managed.

- A disputes rulebook, providing additional guidance to firms on how to deal with common payment disputes using the existing regulatory framework but including the agreed treatment of edge cases.
- Common terminology and coding of disputes across the ecosystem to enable better reporting and more efficiency.
- There was some support also for a centralised dispute management function, although a note of caution was sounded by some who highlighted that the current OBIE Dispute Management System (DMS) has extremely low levels of use, because there had been few disputes and those that had arisen had been resolved bilaterally.

For clarity, these were proposals from a minority of respondents (four, three and three respectively), but there was no counter evidence suggesting these three developments would be unhelpful or not required and we are therefore happy to list these as areas where the evidence provided support.

There was, however, very significant divergence within the evidence submitted during the process. Most of this divergence focused on the scope of disputes, and particularly whether purchase protection should be considered in scope and whether equivalence of protection with cards was required to support the development of open banking payments. There was also divergence on the question of how such protection should be delivered, and whether it could be included within multilateral frameworks or should be delivered as part of the payment rails underpinning open

banking payments (and therefore be provided for all types of transaction running over those rails, not just open banking payments). These discussions are covered in the following sections.

### Area of Discussion 3: Equivalence to cards

Expert advisers were unanimous on this point. One of them commented: *"Consumer protection is, in our opinion, the biggest issue which needs to be solved…"* These experts highlighted the very significant risks, in their view, of open banking payments coming to market without equivalent purchase protections to card. This would create a risk of detriment to end users as well as a risk that open banking payments become reputationally damaged. One of the experts also highlighted that few consumer organisations and commentators would recommend consumers adopt services with what they viewed as significant shortcomings. This submission also highlighted evidence from a firm in the US, which failed to plan properly for the level of disputes it received and has now suffered very serious negative commentary.

Most ASPSPs were typically also of the view that purchase protection was an important consideration. One ASPSP provided an evidence point that allowed us to estimate that chargebacks on debit cards recovered in the region of £400m for consumers per year, suggesting that this protection on existing payment methods is material on debit cards.

However, this view was not universal amongst ASPSPs with one suggesting that purchase protection should be left to individual firms to consider: *"Buyer protection should be left to the competitive space."* This view was echoed by another ASPSP.

Four platforms also supported the view that purchase protection was important, along with one retailer. One of the platforms gave verbal evidence around the issues currently being experienced in relation to disputes in India on an A2A overlay service, which in their view underlined the importance of planning properly for disputes from the outset. The retailer's viewpoint is interesting as it provides a counterpoint to other views expressed by retailers*: "To trust open banking for purchases in everyday categories as well as travel, banks need to provide a dispute process for both fraud and commercial disputes (service guarantees), similar to what is done today with cards."*

However, other retailer submissions disagreed with this point of view, suggesting that the inclusion of equivalent protections to cards would create huge complexity: *"The existing consumer rights are defined and understood, and in turn does not require the complex chargeback rights of card payments."*

As well as this view from a retailer, most TPPs were of the view that purchase protection was not required, and others went further in suggesting that including it would significantly damage the nascent open banking payments market by removing cost advantage against cards.

Many respondents highlighted that customers are protected when making a purchase using open banking payments: they are protected by the Consumer Rights Act 2015 and by various schemes operated within certain industries, such as ABTA and ATOL for travel purchases.

As one TPP set out: *"We should be very careful before replicating the chargeback model as it has created significant costs for merchants and would reduce the ability of open banking payments to provide a better service for merchants."*

Other TPPs also highlighted the extremely low levels of disputes currently experienced within open banking payments today. One for example commented on the *"remarkably low level of payment*

*disputes between customers, merchants, TPPs and ASPSPs. This is not by accident…".* No empirical data was provided to support this point, but a number of TPPs made similar assertions.

**Area of Discussion 4: Where should protection be provided?**

Some respondents who favoured consumer protection, as outlined above, were agnostic on this question or did not provide a view.

Others, however, provided very strong views. One of the expert advisers suggested that this protection should be provided as part of the payment rails, meaning that it would in effect be provided for all Faster Payments. An ASPSP also stated that parity between payment rails was an essential requirement and that a centrally set standard and common functionality for customer protections across all A2A payments would be the best way to achieve this.

Other submissions, more commonly from ASPSPs, suggested that the issue could be solved as part of multilateral frameworks and therefore addressed for open banking payments only and not for other account-to-account payments running over Faster Payments.

**Area of Discussion 5: Allocation of costs**

This was signalled as an important area of debate in a number of responses. Most responses that highlighted this issue did not provide strong views, but rather highlighted that this consideration was fundamental to developing a workable solution to this issue. One example from a platform is typical of comments in this area: *"We note that the inclusion of protection overlay services … adds cost. Where in the value chain the cost falls then becomes the key issue."* Clearly, in the view of this submission and a number of others, the critical question to resolve is, if protection to the customer is provided, who carries the operational costs and who carries the cost of refunding the customer.

**Area of Discussion 5: Consumer Duty**

One of the areas that was highlighted by some respondents is whether and how the new Consumer Duty introduced by the FCA would lead to PISPs providing better advice to customers regarding the level of payment and purchase protection they will receive.

### *1.17.5.2. Emerging Areas of Alignment*

The distinction drawn between payment disputes and purchase disputes was proposed by a number of respondents (although different terms were used) and there is alignment that we should separate discussions of these two types of dispute.

There also appeared to be some alignment around the need for whole of market, centralised dispute management systems, rulebooks and codes of conduct.

Beyond this, this was an area with significantly diverging views, but one of the greatest importance in the views of many respondents.

### 1.17.6. Question 6: Access & Reliability

***Access & reliability: are greater levels of access and reliability needed to ensure success or not? Please provide rationale and evidence. What needs to be done in order to give customers and retailers sufficient confidence that payment journeys are efficient, and payments are certain?***

#### *1.17.6.1. Introduction*

Responses to this question focused on two types of access and reliability issues and for clarity it is helpful to separate these, given that the issues highlighted and potential solutions are quite distinct.

The two issues are:

- **API Availability:** responses here focused on issues of API downtime and occasions when transactions failed because the ASPSP was unreachable.
- **Consent Success:** responses here focused on payments which failed for other reasons, sometimes unknown, sometimes known through error codes. This could include issues such as customer abandonment, technical faults, failed authentication, etc. We have tried to keep issues related to high-value transactions separate, given that these are clearly addressed under Question 1 (Resolving Barriers). We have also kept functional enhancements separate, as these are considered under Question 4 (Functional Capabilities), such as error codes or issues related to payment status or payment certainty.

Some respondents referred to their views around API Availability, some around Consent Success, and some both. Other responses saw limited evidence of gaps or issues in either area. However, for clarity, and to aid decision-making by the Committee, we have separated evidence and proposals into these two areas.

#### *1.17.6.2. Areas of Discussion*

**Area of Discussion 1: API Availability**

There was partial agreement that API Availability was a gap that needed to be considered by the Committee and that the issues of API Availability needed to be resolved to achieve the long-term success for open banking payments. In total, 14 submissions highlighted issues in this area, which needed to be addressed, although some did consider this to be a long-term issue, rather than a short-term priority.

Participants that supported action of some type in this area included two ASPSPs, four platforms, two expert advisers and six TPPs. As can be seen therefore, there was support from across the ecosystem. A further three responses stated that high API availability was essential but did not go as far as saying that the current performance was inadequate.

Some of the evidence cited included:

- A platform highlighted that the current level of performance of the CMA9 Banks equated to 44 hours of downtime per year.
- A TPP highlighted that *"7% of the failed payments were caused by "problems connecting to the bank",* making it clear that API availability represents a small proportion of failures but still a significant number if open banking payments is to scale.

- Another TPP highlighted that they had observed, “One bank had 13 downtime events over the course of 12 days, during which time our payment conversion rates dropped from 52% to as low as 8% on a seven-day moving average.”

Many respondents compared the current level of availability (targeted at 99.5%) with that of the cards ecosystem (which is typically 99.99% available). One of the expert advisers suggested, *“API availability and reliability must be increased so that it at least matches the performance of other payment methods with which open banking payments are competing.”*

- One ASPSP referred in its submission to the fail-over systems employed in the cards ecosystem to stand in for bank systems when they are down. This bank had a system outage for about four hours and used the payment scheme’s Stand-In Processing. During this 4-hour period, 2.5m debit transactions, worth over £120m were processed on behalf of the issuer.

To counterbalance this view, however, two TPPs, one platform and two ASPSPs explicitly stated the current level of availability was sufficient and no further work was required. One TPP stated that, *“the UK user experience is relatively efficient and performs well.”*

Whilst we can observe partial agreement that API availability is a key gap for many respondents, there is much less clarity or agreement on the type of solutions which could be deployed to bridge this gap. Many submissions did not include specific recommendations. Those that did, diverged on what kind of solutions would be appropriate. Some of the key solutions proposed included:

- A number of respondents made recommendations about harmonising the treatment of providers subject to the CMA Order with that of all other ASPSPs. For example, one ASPSP proposed that all ASPSPs should be targeted to provide 99.5% availability and suggested that the PSD2 requirement of parity was insufficient. Two TPPs called for all ASPSPs not just CMA9 providers to provide monthly reporting of API availability.
- One platform and three TPPs made representations that an API-based tool should be created which allowed TPPs to understand exactly which APIs were operational and which were not in real-time, *"a whole-scheme availability dashboard that gives real-time updates on all participants".*
- One proposal for consideration was a formal, stand-in processing capability which was able to authorise transactions on behalf of the ASPSP if their systems were down. Respondents did not provide details of how such a system would work, but many appeared to have in mind a solution similar to that which is operated in the cards ecosystem. One TPP, three ASPSPs and one platform proposed solutions of this type.
- One ASPSP pointed to other critical infrastructure such as the Open Banking Directory and suggested that this should be developed to have fail-over capability as it represented a single point of failure for the ecosystem.

As is clear from the analysis above, a number of respondents did not put forward recommendations for fixing the perceived API availability issues which they considered should be addressed by the Committee, suggesting that further work may be required to understand potential solutions and assess their proportionality and effectiveness.

### Area of Discussion 2: Consent Success

This section considers submissions to this question which focused on access and reliability issues experienced by participants where the bank API channel was available, but the payment still failed. We have referred to this as “consent success”, however we should also highlight that aspects of this

issue are also contained in Question 1 (Resolving Barriers), particularly consent success for high-value transactions, and Question 4 (Functional Capabilities), as it relates to payment certainty.

In total, nine organisations highlighted that issues of consent success represented a gap that needs to be overcome. These nine respondents included five TPPs, one bank operating as a TPP and three platforms.

For example, one platform highlighted that *"over 21% of payments initiated appear to have been retried at least once suggesting there are high failure/abandonment rates as journeys progress".* Another platform quoted data which showed that: *"Drop-offs during the ASPSP side journey occur in 31% of payment journeys for all banks to which [TPP] is connected (NB: this excludes payments which failed for technical reasons which is typically around 4%)... The range among CMA9 banks is between 23% and 52%. However, for non-CMA9 banks, it is between 11% and 85%. A robust, uniform approach would therefore increase reliability."*

Two ASPSPs however were clear that there were no issues here and that the current consent success rates were a natural function of consumer behaviour and did not present a barrier to success. For example, one ASPSP noted that: *"Conversion rates for open banking payments are greater than 90% (consumers successfully authenticating a payment)"*. Another noted that, *"… there have been significant improvements in conversion, made through continual review and enhancements to our app and browser journeys".*

There was also no clear view from the submissions on actions which should be taken if the Committee were to address this gap. In total nine submissions raised issues in this area, only three proposed solutions. This may be because respondents did not consider that this was in scope of Question 6 and others considered that some of the proposals put forward to Question 1 (Resolving Barriers) and Question 4 (Functional Capabilities) would have an impact on consent success rates.

Three respondents recommended that a whole of market reporting and issue resolution solution be created, noting that the OBIE is only able to address issues related to CMA9 implementations.

As evidenced in a number of submissions, consent success is a simple concept, assessing whether a payment has been successful or not, but has a number of very complex drivers, including technical issues, consumer drop-off, quality of implementations, payment limits and fraud. Therefore, responses to this question also need to be considered alongside responses to other questions, in particular Question 1 (Resolving Barriers) and Question 4 (Technical Capabilities).

#### *1.17.6.3. Emerging Areas of Alignment*

On balance, the evidence provided suggested that API availability is a gap which needs to be addressed to unlock the potential of open banking payments, however for some respondents this is a longer-term issue rather than an immediate priority. There were, however, important dissenting voices on this question.

There was limited alignment on how such a gap should be addressed however, partly because many responses did not even consider what kind of solutions could be deployed in this space.

On the question of consent success, there was limited alignment about whether this was a gap needed to be addressed or not and what solutions which could be deployed in this regard.

### 1.17.7. Question 7: Pricing

***Competitive pricing: in terms of commercial models for the use cases, what are the challenges with current charging models, and how can competitive pricing be achieved in a fair manner that incentivise actors to take part?***

#### *1.17.7.1. Areas of Discussion*

There were very wide-ranging views expressed regarding pricing. This is not surprising as open banking payments is a two-sided market and the different parties across the system derive commercial benefit from separate drivers, for example ASPSPs incur a cost for every payment initiated over open banking, but if there is a cost to PISPs for payment initiation this undermines the ability for them to provide a credible alternative to existing payment methods.

**Area of Discussion 1: Pricing of non-Sweeping VRPs**

This was the area of least divergence with several ASPSPs and several TPPs suggesting that a commercial model which provides a return to ASPSPs for open access to VRPs was appropriate. This was seen as akin to the activities taking place in Europe as part of the SEPA Payment Account Access (SPAA) initiative. Several of the TPPs suggested that regulatory intervention may be required to set the price or cap the price with many stating that the cost would need to be below the cost of debit interchange to ensure there was an incentive for merchants to adopt this new payment capability. However, there were also calls for free access to VRPs for any use case from TPPs, retailers and expert advisers. The retailer and expert adviser submissions suggested that interchange on card transactions should be abolished, removing the incentives of ASPSPs to continue supporting card transactions and not invest sufficiently in the development of open banking payments.

**Area of Discussion 2: Pricing of all open banking payments**

Seven ASPSPs referenced the cost associated with open banking payments with five respondents directly or indirectly recommending a charging model that will allow them to be compensated for these additional costs, i.e., a charging model for all open banking APIs currently with open free access. This model was not suggested by any TPPs.

**Area of Discussion 3: Other observations**

One TPP recommended that any agreements on pricing could be part of a broader Payment Arrangement which would cover commercials, liability, customer protection, conformance and performance. This would enable direct oversight by the PSR and could cover VRPs as well as Single Immediate Payments (SIPs) initiated in open banking. These Payment Arrangements with better

performance and customer protection could sit alongside existing APIs developed to meet a regulatory obligation.

Whilst most TPPs who responded that some form of commercial model for VRPs needed to be cheaper than Direct Debit to promote switching. Some of these TPPs cited that the reference point for cost should be Direct Debits rather than debit card interchange. One payment network sought clarity around what costs should be compensated for, which can include costs of processing the payment request/costs of handling disputes and consumer protections/costs of sending the payment (processing and FPS fees).

#### *1.17.7.2. Areas of Potential Alignment*

This was an area with very clearly divergent views across the ecosystem.

### 1.17.8. Question 8: Other Comments

***Are there any additional issues pertaining to open banking payments that you wish to raise that are not covered in the preceding questions?***

Twenty-three respondents did not provide any additional comments.

Three respondents highlighted the importance of considering the role of the NPA in decisions relating to the future of open banking payments.

Other respondents used this section to highlight important considerations for Phase 2, including suggestions that it should focus on the commercial structure of the Future Entity and a deeper consideration of the needs of consumers and merchants.

Other submissions used this as an opportunity to restate priorities set out earlier in their submission.

## 1.18. First Data Strategy Sprint

### 1.18.1. Question 1: Preventing Fraud

***What additional data could be shared between entities to better protect customers from fraud, in particular APP fraud, for account-to-account payments (beyond the realm of open banking payments)? Please provide rationale and evidence.***

***Additional clarification: This question covers all account-to-account payments, not just payments involving a PISP and seeks to understand what data could be shared using APIs between trusted parties.***

#### *1.18.1.1. Introduction*

There are widely differing views of the materiality of fraud risks created by open banking, which influenced the extent to which respondents considered increased data sharing as a priority. A key issue identified across the board is the paucity of good empirical data to inform this discussion. Most respondents suggested that the starting point to address this gap was to identify how existing data collection initiatives could be used more effectively rather than the creation of new workstreams.

Note that this question, although part of the Data Sprint, principally focused on preventing payments fraud. Therefore, there is additional relevant information in responses to Question 1 from the Payments Sprint. See Section 4.1.2.

#### *1.18.1.2. Areas of Discussion*

**Area of Discussion 1: The role of additional data**

The majority of TPPs expressed the view that across the ecosystem, all participants share a common goal of protecting customers and stopping fraud from occurring. Many TPPs suggested that receiving certain new data points would improve their risk profiling capability. Most TPPs stated that they were receiving insufficient customer attribute data that would enable them to better identify payers and beneficiaries. Six TPPs indicated that it would be beneficial to receive:

- Name of account holder (rather than account name)
- Opening date of account
- Account holder date of birth
- Account holder address
- Business entity details (i.e., business name, address, tax ID)

Many ASPSPs were wary about requiring expansion of data points, noting that GDPR requires a lawful basis of processing data based on data minimisation principles. Therefore, they considered defining a wide data set up front without assessing whether sharing is necessary may be problematic. One ASPSP noted that the overhead of sharing very prescriptive data was very high, although acknowledged the benefits of being more open and collaborative.

All of the ASPSPs indicated that they felt that the TRIs recently introduced into the Open Banking Standards represented a good starting point, but that it is important to create an agile way to react to novel emerging fraud trends.

The role of Confirmation of Payee (CoP) was an important topic for one TPP, who was concerned about the additional friction such calls could bring and made a case that TPPs should be responsible for undertaking CoP checks.

### Area of Discussion 2: Reducing Account-to-Account Fraud

ASPSPs referenced the API-based EFDS being developed via UK Finance in their responses. It is intended that this will allow ASPSPs to exchange account level-data that allows the sending bank to risk profile transaction prior to sending payments or the receiving bank potentially to restrict customer access to funds based on assessment of relevant data points. A Proof-of-Concept that was undertaken earlier this year identified five particular new data points that are considered relevant:

**Purpose of a Payment**
**Age of Account Holder**
**Tenure of Account**
**Turnover of Receiving Account**
**Type of Account**

Evidence was submitted indicating that the Proof-of-Concept evaluation clearly demonstrated that if these data points were shared between the sending and receiving banks fraud detection rates might improve by c. 20%, which based on current APP fraud losses could produce a potential reduction of c. £120m pa.

The potential for improvement in inter-bank risk management was thought likely to reduce the need for TPPs to make significant changes to their existing risk scoring approaches. One TPP stated that an "*API-based EFDS that will allow ASPSPs to exchange additional information about a payment before it is executed. We recommend that JROC supports these efforts and encourages the development of further information exchange between the ASPSPs, without requiring a payment initiation service provider (PISP) to be involved.*"

However, the one area in which TPPs are likely to be required to support this new approach is in identification of "payment purpose", which is key information that they hold in an open banking payment. One ASPSP stated that "*understanding fully the purpose of the payment (who the customer thinks they are paying and for what reason) is both the most critical but also the most difficult to obtain*". The existing TRIs in the Open Banking Standard aim to provide this key information to the sending bank.

An ASPSP indicated that from an open banking payments perspective, the anticipated outcome was that the additional data flow can in fact result in less transactions being declined or investigated in some cases (i.e., reducing false positives).

A TPP highlighted the need for clarity on outcome, so that customers were clear what was happening if their transaction was delayed or stopped, a topic discussed in the Payments Sprint.

One ASPSP suggested that data sharing by providers outside of financial services, e.g., telecoms and technology platform providers, would also improve fraud outcomes.

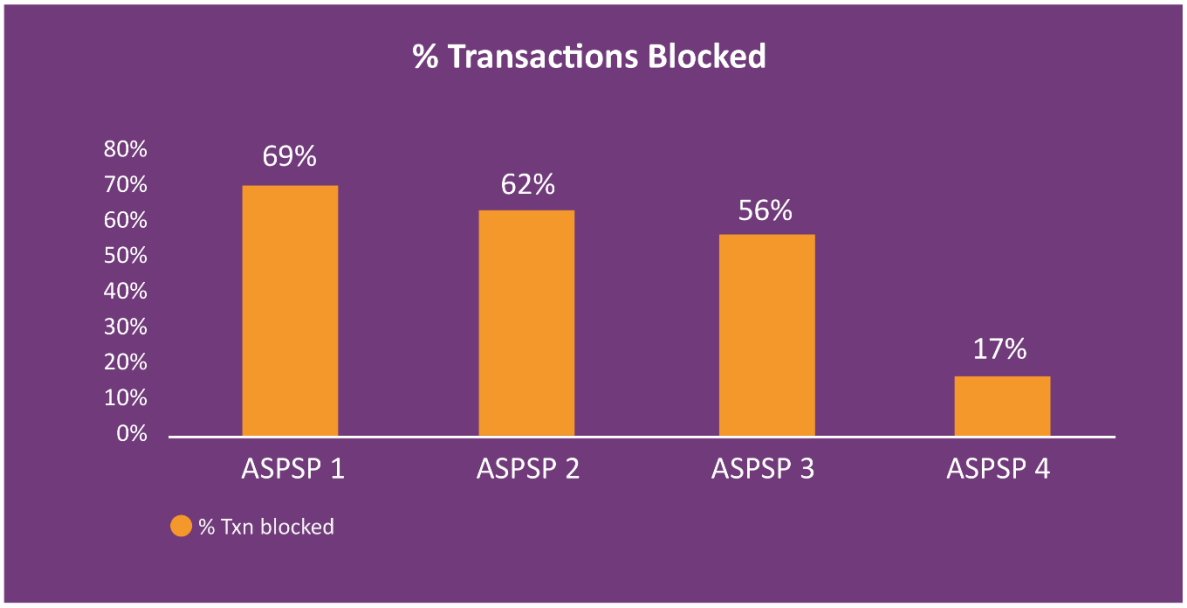
### Area of Discussion 3: The extent of fraud in open banking payments

There are differing views on the extent to which the fraud risk in open banking payments is substantial. TPPs argued that open banking payments were inherently low risk as evidenced by the fact that they currently generate very low levels of fraud. However, ASPSPs refuted this view and suggested that from their perspective fraud rates were proportionately higher than those on their

direct digital banking channels. One ASPSP indicated that fraud losses are five to ten times higher (although noted that the volumes of payments are markedly different between the two channels). The low levels of friction in open banking payments and the lack of visibility as to the purpose of the transaction and the participants involved were identified as contributing factors.

One TPP suggested that many ASPSPs' fraud-scoring capabilities were poor, generating a high level of false positives. The TPP provided evidence that considerable numbers of payments had been blocked as suspected fraud, an increasingly common trend. The proportion of all payments blocked in the first week of September as experienced by the said TPP is set out in the figure below.

***Figure 4: Evidence Supplied by a TPP: % Transactions Blocked***




The TPP indicated none of these transactions was proven to be fraud, and the majority of these were individuals transferring cash between accounts in their own name, between accounts that had been set up for a long time and for amounts that were not unusual.

One ASPSP observed that the existing largest use cases for open banking such as paying tax bills, paying credit card bills, or topping up a secondary account, are not big drivers of fraud. However, as the use of open banking payments evolve, other potential use cases may introduce new risks. Data sharing capabilities needs to reflect future potential risks, not just existing ones.

### Area of Discussion 4: Role of PISPs in fraud management

A few TPPs in the discussion session held on 30 September 2022 challenged whether additional activity was required given the low levels of fraud and risk created by open banking payments today. The majority of TPPs called for a two-way data sharing ecosystem to improve risk scoring capabilities covering both data to be shared from ASPSP to PISP, as well as data from PISP to ASPSP. The PISPs have access to transactional data, e.g., information on payment purpose but very little data relating to the attributes of the account or account holder. ASPSPs and some TPPs noted that banks (both receiving and sending) have the benefit of holistic customer payment behaviour data that means

that they are much better placed to detect unusual high risk transactional activity than PISPs, who only see occasional transactions. Several ASPSPs also noted that because they had ultimate liability for fraudulent transactions, they were better incentivised to undertake risk monitoring.

However, one ASPSP noted that understanding the purpose of the payment (who the customer thinks they are paying and for what reason) is one of the most critical but also the most difficult to obtain. They thought that PISPs would naturally have a key role to play in providing this particular data element.

#### *1.18.1.3. Emerging Areas of Alignment*

Given the conflicting perspectives as to the level of fraud and the level of risk associated with open banking payments, most participants agreed that having empirical data sets on fraud would be essential to resolve conflicting views on how much fraud is being generated via the open banking channel. This should include evidence of the type and volume of fraud being reported. This was identified as a prerequisite to considering what new data could be brought into play, and who should supply it.

On the specific question of improved data sharing in relation to account-to-account payments, there was broad agreement that this is an important opportunity to address a significant source of fraud, with broader benefits for the ecosystem. ASPSPs recommended that the Committee considers the work that is underway in relation to the API-based EFDS before progressing other data sharing initiatives.

### 1.18.2. Question 2: Ways to share data

***Should the ecosystem consider the use of risk indicators and software statement or not? Please provide rationale and evidence. How would that affect any friction in customer journey?***
***Additional clarification: This question seeks to investigate ways in which different data sets are / could be shared between parties in relation to risks / to mitigate risks in the payments / data chain (e.g., using software statements, using risk indicators in the payment initiation data flow, other ways) and the relevant rationales for different approaches.***

#### *Introduction*

The starting point for all respondents is that there is shared appetite across the whole ecosystem to reduce fraud. However, it is evident that in practice there is mistrust on whether or how that data is used between parties. There is evidently an appetite on the part of all participants to improve the effectiveness of risk-scoring utilising appropriate data, but some divergence on how this is to be achieved.

#### *1.18.2.1. Areas of Discussion*

**Area of Discussion 1: Role of risk indicators in fraud reduction**

ASPSPs universally welcomed the modification of TRIs as part of the Open Banking Standard (v3.1.10). They stated that the existing TRI data points provide the right contextual information to make better informed and risk-based decisions, which would improve fraud detection and reduce the number of declined payments, resulting in an improved customer and merchant experience.

However, their concern is that TRI data is not consistently and accurately populated by PISPs. Partial adoption (as currently seen) makes it difficult to exploit the data. Not only should TRIs be invariably used, but the data supplied should be consistent and accurate. For the quality of TRIs to evolve, it is important that they become embedded across the ecosystem so that their effectiveness can be determined, and improvements made. Further development of these controls relies on having reliable data from across the ecosystem to understand the risk levels.

Several TPPs acknowledged the importance of the use of TRIs and recognised that the success of fraud controls within the ecosystem is materially dependent on consistent implementation.

Two TPPs expressed concern that single data points provided in the TRIs might be used as an absolute to determine if a transaction is legitimate, rather than it being considered as one of many factors and stated that "*no single data point can absolutely determine whether or not a transaction is fraudulent, so it's important that any analysis of whether a transaction is legitimate must keep this in mind and not operate in absolutes*".

**Area of Discussion 2: Achieving comprehensive TRIs**

While there was broad agreement around the essential need for a standardised implementation of TRIs and mechanisms to ensure that they were invariably and consistently used, there were differing views as to how that should be achieved. Version 3.1.10 of the Open Banking Standard allows PISPs to share more risk data about the nature of the payment being initiated and the payee to assist the sending bank in assessing the risk of fraud. However, this is optional for TPPs and while the

implementation of TRI capability is only mandatory for CMA9 ASPSPs, the Standard is silent on the use of them in ASPSP fraud engines. There would be significant benefits to the ecosystem if there were a requirement for TPPs to share TRIs and for all ASPSPs to use them.

Most of the ASPSPs indicated that it should become a mandatory requirement for PISPs to use TRIs, with clarity on mandatory and optional data elements. A commonly held view was that there was a need for a governance framework and rules that ensure TRIs are populated and rules applied across the board. One ASPSP alternatively suggested that TRIs could be implemented via MLAs. This submission suggested that implementing TRIs via an MLA would provide effective incentives for PISPs to provide good quality TRIs and for ASPSPs to make risk-based decisions based on those TRIs and to invest in their risk engines.

TPPs unanimously agreed that TRIs, if well implemented, can be beneficial to avoid indiscriminate payment failures that occur when a blanket approach to fraud prevention is applied by ASPSPs, and agreed that there needs to be central coordination of how TRIs are implemented. They suggested that it should be undertaken by the Future Entity, but did not specify how this could be achieved.

### Area of Discussion 3: How can permissions clarity be achieved to identify how data is being shared and used?

From a transparency perspective, there was consensus from respondents that it is desirable for both ASPSPs and their customers to know the recipient of their data or the merchant that they are dealing with. This is currently not the case. Although there is an existing solution, intended to achieve this, where agents of AISPs and the beneficiaries of PISP payments should be identified in 'on-behalf-of' fields of a software statement. There was universal acceptance that currently this is not being done in many cases.

The vast majority of TPPs stated that the reason for this is that the process of creating separate software statements for every business who uses open banking payments/ data, is very cumbersome. They indicated that managing multiple software statements incurs a sizeable overhead for TPPs and introduces significant risk of data being incorrectly maintained and out of date. Some TPPs indicated that the current approach is not scalable for handling the large numbers of merchants as the use of open banking payments grows. The majority of TPPs noted that this is now of additional importance as VRPs are being rolled out, so that consumers can accurately identify their payment mandates on their banking app.

### Area of Discussion 4: Lack of permissions clarity

Discussions in this area focused on whether the current system of software statements used within the Open Banking Standard provided sufficient clarity on who consumers had provided consent to or who the ultimate beneficiary of a payment was.

There were divergent views as to whether the limitations of the current model presented a significant ecosystem risk. An ASPSP provided evidence that in a recent incident the inability to accurately identify the parties in the data sharing chain had hampered their ability to effectively manage risks posed to end-users. Two other ASPSPs stated that this creates a potential ecosystem risk because in the event of a data breach it would not be possible to determine which customers may be at risk because there is incomplete view of how data is being shared and used.

Several ASPSPs noted that while more granular information would allow them to better assess the risk associated with a specific merchant it was considered a fairly blunt tool when assessing transaction risk.

**Area of Discussion 5: Achieving permissions clarity**

The key area of divergence was around how improved clarity is best to be achieved.

With few exceptions, ASPSPs submitted evidence that the current solution (utilising software statements) is suitable and that they are able to accept a large volume of software statement registrations. The proposed alternative (identifying parties in the consent journey) would involve significant delivery for ASPSPs to implement, without any clear immediate benefit to customers or merchants.

Two ASPSPs expressed the view that the current solution (the use of software statements) is fit for purpose and that the efficiency of it could be improved. This would, in their views, address many of the issues identified as a barrier to adoption and would require a one-off investment to resolve. Completing software statements accurately was considered by these responses as a "cost of doing business" in a way that benefited all parties in the chain, including the end customer.

Most ASPSPs, while somewhat sympathetic to the issues raised by TPPs, noted that the use of software statements has been a fundamental part of the open banking ecosystem and changing to a new mechanism would be a material change that would require significant development for both ASPSPs and TPPs. They noted that there was an absence of any clear immediate benefit to customers or merchants, the primary driver being reduction of costs and effort for TPPs.

Only one TPP agreed that, from a technical perspective, the proposal to move to the suggested new approach could add complexity and significant costs for both TPPs and ASPSPs. The majority argued that replacing software statements (for example, where the *consent token* is used to display who the customer is dealing with) as the means to identify the customer facing entity in bank dashboards is essential.

#### *1.18.2.2. Emerging Areas of Alignment*

From a counter-fraud perspective, there was unanimous agreement that the adoption of TRIs and the more consistently they are implemented, would lead to improvement in the ecosystem, less friction in the customer experience and ultimately better consumer outcomes. This would enable not only better fraud detection but also to prevent false positives, where genuine payments are blocked. Improvements in this area will have a consequential positive impact for open banking payments.

There is good consensus that better coordination is required to facilitate this, but further consideration needed as to how exactly to achieve this and whether rules or regulatory intervention is required. Achieving permissions clarity transparency is a desirable outcome, irrespective of the extent of ecosystem risk. There may be a case to migrate from the current approach to an alternative, but more work is needed to assess the problem, evaluate alternatives and assess the cost benefits case, including the balance of development costs between parties.

### 1.18.3. Question 3: Sharing identity

***Can sharing identity detail through open banking help and support the payments / financial services ecosystem? Please provide rationale and evidence. What are the use cases and models that could thrive? Are there barriers to adoption and if so, how do we address those?***

### *1.18.3.1. Introduction*

Digital identity is a complex area, and some respondents did not provide a response in this area and others provided short, high-level responses. However, there were a number of thoughtful, detailed responses.

Throughout the sections below, a distinction is drawn between the sharing of identity, referring to a full identity proving service, and the sharing of identity attributes, which could include data fields such as address or date of birth, which could be used by others to check identity.

### *1.18.3.2. Areas of Discussion*

**Area of Discussion 1: Use cases of identity services**

Many respondents listed a number of ways in which the sharing of identity attributes through open banking could deliver new or enhanced experiences or/and address underlying issues. Most suggestions could be clustered into the following two areas:

- Reducing risk or enhancing payments by the sharing of identity attributes to PISPs or sending banks. The opportunity to use additional data to better manage fraud is considered under Question 1 (Preventing Fraud), but there are additional opportunities in this space. Seven respondents highlighted opportunities in this area including TPPs, platforms and ASPSPs. This could include, for example, providing address or contact details to allow pre-population of check-out details, or an age verification service.
- Reducing the friction associated with account opening, KYC or onboarding. This is a complex process for many providers, with the hassle being passed to customers and the cost born by the provider. The sharing of identity attributes was identified by eight respondents, mainly from the TPP community, but also including two ASPSPs.

Some other opportunities were less broadly cited, but are worth setting out here. For instance, a respondent suggested that the sharing of identity or identity attributes could act as a catalyst for innovation and the creation of new propositions.

One respondent drew on experiences in the alternative credit market. This submission provided evidence that many lenders find it hard to prove the identity of many of their vulnerable or excluded customers. For example, this respondent highlighted an example where 36% of customers failed Identity and Verification (ID&V) because these customers had thin credit files or a limited file with Credit Reference Agencies. As this respondent notes "*exclusion leads to further exclusion*". Many of the target customers of such lenders do not have passports or driving licenses. Another submission quoted data that, "*5m UK consumers are still classified as 'credit invisible' - people with little or no credit history. This reduces their access to mainstream financial services*."

There was therefore a call for *"mainstream banks [to] help… to support a financial services ecosystem for consumers that are currently excluded from mainstream finance".*

However, one response identified very limited opportunities from identity sharing through open banking. They suggested, *"We should allow the market to develop propositions through a cross-sectoral model (rather than creating a 'separate' model through open banking rails that could be relatively financial services specific)."* A number of responses highlighted other initiatives in the Digital ID space and urged caution (see below).

### Area of Discussion 2: What models are identified?

Four main models were identified in responses.

- The first is that additional attributes are shared by ASPSPs with TPPs, primarily to help with KYC, onboarding and to reduce friction. Suggested data fields included address, contact details, date of birth or information about KYC undertaken. This was widely proposed by the TPP community, with seven TPPs calling for it. Only one ASPSP explicitly proposed this as an opportunity.
- The second, and closely related model, is the sharing of data to entities initiating payments. This could be data to help such entities identify risky transactions prior to initiation (which is considered specifically under Q1). Others highlighted that potential time-saving benefits of providing address, contact details or age verification to reduce friction and manual form-filling during PISP journeys. One ASPSP explained the opportunity as follows: *"We have identified use cases combining attribute sharing with payments. The details are commercially sensitive but generally relate to smoother journeys with less customer data entry e.g., at checkout, and verifying attributes such as addresses and ages."* Such opportunities were proposed by four ASPSPs, a platform and one TPP.
- The third model was the creation of a digital identity or 'authentication as a service' allowing entities in other, unrelated sectors to use ASPSP authentication. This was only suggested by four respondents.
- Two ASPSPs were keen to highlight that rather than simply acting as an attribute service provider, they too would benefit from ability to access attributes from other entities, such as HMRC or other Government departments.

Finally, although it is not a separate model, it is worth spelling out the opportunity identified for consumers with thin credit files and limited ability to prove their identity, as described above. This challenge is very real and acts to exacerbate exclusion. This model is in effect an application of the first model mentioned above but tackling a real and pressing need in the market to broaden access to the financial services market. One ASPSP also identified the role that expanded data sharing could play in supporting such customers: *"Wider data points could be used to offer more lending to those in vulnerable circumstances or with limited traditional credit reference data to avoid them being forced into high-cost credit scenarios."*

Looking at the pattern of responses, it is quite striking that there is a broad appetite amongst the AISP community to consume additional identity data from ASPSPs through open banking. ASPSP responses are more circumspect, with many highlighting challenges set out in the section below. Only one response from an ASPSP was directly opposed to this idea, however.

On the other hand, in the payments market, there appears to be some appetite amongst large ASPSPs to provide additional data to PISPs to enhance payment experiences and make them more convenient for customers. We have not received many submissions from the TPP community expressing this as an opportunity. This may be partly explained by the relatively small number of PISPs on this panel, and it is worthy of further consideration by the Committee.

### Area of Discussion 3: Barriers

We received a small number of very detailed responses on barriers to providing identity attribute sharing models. There are a number of these barriers highlighted.

The most commonly cited barrier to progress with an open banking identity solution is the well advanced, complex and fast-moving Digital ID market in the UK. Four ASPSPs highlighted the various schemes in flight, the work being undertaken by DCMS, and all expressed concern about how an open banking solution could fit into that complex picture. One platform is actively involved in a proof of concept already and was keen to ensure that any open banking initiative was complementary to this. One ASPSP submission summarised this viewpoint well: *"There are already several digital identity schemes developing – for example, TISA, OneID and MyIdentity. Complexity is an issue with too many competing approaches. We strongly encourage alignment of any further related work to DCMS/government efforts."*

The second challenge highlighted by one expert adviser and two ASPSPs was that the KYC attributes that the market is so keen to consume may not be reliable. For example, one ASPSP suggested, *"When assessing bank-held identity against Good Practice Guide 44/45 a medium level of confidence is reached."* The reason for this was explained by the independent expert: *"As the ASPSP data is normally based on third party data (e.g., the account owner's passport when they opened the account) rather than being an authoritative source in and of itself (e.g., database of valid passports), then important meta data about the checks undertaken probably needs to be shared as well."*

A third linked challenge therefore presents itself, although this was only highlighted by two ASPSPs and the independent expert: the challenge of liability if an identity attribute proves to be unreliable and leads to a loss by the relying party.

The next challenge was highlighted by two respondents, which is the commercial framework for any identity attribute sharing model. None of the TPP responses mentioned a commercial framework. It is hard to draw firm conclusions about the expectations here. Either TPPs hadn't considered a commercial framework, or they had an expectation of this data being provided on the same basis as existing PSD2 data (i.e., free and open access).

Two respondents highlighted the challenge that consumers must be clear on what data is being shared and for what purpose.

One respondent also highlighted that for the payment models to work, a combined consent covering payment and data would be required. Their view was that would require changes to the Payment Services Regulations.

One challenge was highlighted by an ASPSP which described solutions in this space as a "network play", meaning that it would only work if sharing of data attributes was ubiquitous across the market. A TPP would be unlikely to change their business processes to use such data if it was only available from one or two ASPSPs.

The final challenge was provided by an ASPSP, who commented that work on Extended Customer Attributes had been undertaken by the OBIE. To date this has not seen any take-up and this respondent encouraged the Committee to consider why there had been limited progress before embarking on future initiatives in the space.

#### *1.18.3.3. Emerging Areas of Alignment*

There is widespread appetite in the TPP space for additional identity attribute sharing by ASPSPs and only one ASPSP is opposed to this concept (suggesting that this should be left to other Digital ID initiatives). Assuming that some of the barriers can be addressed (e.g., commercial framework, reliability of data, ubiquity, fit with other Digital ID initiatives) there would seem to be potential for the expansion of the open banking ecosystem to include some additional identity attributes.

ASPSP submissions show strong support for identity attribute sharing to enhance payment journeys in particular. TPP support for this is less clear, but as a caveat we would highlight however that we have relatively limited input from PISPs to this question, which may reveal greater appetite. The fact that one ASPSP is already working on a pilot in this area suggests that the evidence of appetite may be understated.

The barriers set out by some of the ASPSPs and the independent expert are considerable, however, and should not be under-estimated. Surprisingly, few TPP responses highlighted these barriers, suggesting a difference in perspective on this topic. TPP perspectives are quite straightforward: they see a need for additional data and can identify how it would help reduce friction, support innovation and address exclusion. Bank perspectives are more nuanced, having been involved in a number of Digital ID initiatives and perhaps with greater awareness of the challenges, nuances and barriers.

### 1.18.4. Question 4: Vulnerable customers

***What are the new use cases that could be developed to benefit consumers in vulnerable circumstances (e.g., in situation of bereavement, limited access to credit, aggravated by cost-of-living crisis etc.)? Please provide rationale and evidence.***

#### *1.18.4.1. Introduction*

A number of responses highlighted the importance of developing strategies to support vulnerable consumers, highlighting that FCA guidance requires outcomes for vulnerable consumers to be as good as for non-vulnerable consumers. Others highlighted the very broad range of vulnerabilities and cautioned against thinking of vulnerability as a "type" of customer, but more a phase through which most people will pass at some point in their life.

Two responses highlighted that the question assumes that open banking will be a positive force for consumers in vulnerable circumstances. The majority of evidence supported this view, but these two responses urged caution, reminding the Committee that open banking may also *"inadvertently increase risks"* for some consumers.

#### *1.18.4.2. Areas of Discussion*

**Area of Discussion 1: Most valuable opportunities**

A very wide range of potential services were highlighted in evidence, and we list these in order of the number of responses which highlighted the opportunity.

- **Additional data to help apply for credit:** in total 11 responses highlighted the benefits that open banking data can bring when consumers are applying for credit, by allowing lenders to see other aspects of their financial situation such as regular payment of rent or other bills. This is data which is not available to Credit Reference Agencies and may therefore help to prevent vulnerable consumers being forced to go to high-cost credit providers. A further four submissions highlighted a related, but distinct, area which was to help consumers with very limited digital identity, who fail traditional identity checks and therefore can be excluded from lending or savings products. (See above for additional information, Question 3, Sharing Identity)
- **Providing a broader view of assets and liabilities:** eight submissions supported the expansion of data available so that TPPs could provide fuller and more accurate overviews of vulnerable consumers' financial position. This could be to support better advice, for example in a debt advice journey, or simply to help provide better PFM style dashboards bringing all financial holdings into one place. As one TPP submission stated: *"The next logical (and urgent) step is Open Finance. Only when we open up smart data across the economy will truly transformational benefits for customers be realised."*
- **Enhancing SME lending:** four submissions highlighted opportunities to support SMEs in applying for and shopping around for credit, showing that we shouldn't consider vulnerability to be only relevant for consumers, but for small businesses too.
- **Simplification of bereavement processes:** coping with bereavement can place many consumers into vulnerable circumstances, but also presents significant logistical challenges. Four ASPSPs saw scope for open banking to support consumers through this process, for example through tracking down digital accounts owned by the deceased.

- **Accessing other people's accounts:** four responses highlighted situations where a vulnerable consumer may want others to access their account, either as part of a formal Power of Attorney or Power of Guardianship scenario, or as part of a broader support network. An independent expert provided evidence of how common this can be, with research showing that *"half of those who care for someone with a mental health problem know someone else's PIN number (52%), 27% have used someone else's contactless card and 23% know someone else's online banking password".* These kinds of arrangements are therefore very common, but are high-risk, break terms and conditions, and leave the vulnerable person open to harm. Open banking could provide a better, more formalised, lower risk method of sharing the burden of managing money.
- **Open up access to accounts beyond financial services:** four responses highlighted important opportunities for pulling in data from providers such as energy companies or HMRC. Two of these responses talked about the opportunities for automated sweeping into energy accounts, for example sweeping additional funds across to build up a cushion against rising bills. One provided evidence that, *"In our exploration for those in financial distress, we have found that access to non-financial data sets is now the most compelling way to offer new products and services to customers. So, for example, wider access to energy and utility account data would assist customers in getting a better deal and help them create financial headroom and develop their financial resilience."*
- **Automated benefit eligibility** was an opportunity highlighted by four respondents. One independent expert provided a case study from a lender using open banking to help its customers identity missing benefits. This lender launched the service in January 2022 and found that 68% of their customers were missing out on benefits they were eligible for worth on average £5,088. These services could be much more effective with additional data sharing, such as postcode however to improve matching.
- Another area was **providing more control over recurring payments**. Three responses from the TPP community highlighted the additional control of VRPs as compared to recurring card transactions.
- Two responses highlighted the ability to **identify potential signs of vulnerability**, meaning that a TPP, with the broader data and insights available, may be able to identify when a customer is becoming vulnerable. In a related point, two submissions highlighted that by making it easier for consumers to see their overall financial picture, they may be able to identify their own vulnerabilities. One TPP submitted evidence of *"feedback … from a customer who had not appreciated how much they spent on gambling until they had seen their consolidated financial position across all accounts... This customer wrote… to thank us for providing a view of their spending which has now changed their behaviour."* Four submissions suggested that there may be scope to share such vulnerability information (with consent) with other parties within the ecosystem. One ASPSP however disagreed with this, due to the significant GDPR obstacles of sharing such sensitive data about people.
- **Ongoing monitoring of lending** was identified by two respondents, who highlighted that a lender with ongoing AIS access can monitor their customers more effectively and ensure that lending remains affordable.

Most of the examples above are proposals or ideas for new or potential services that could be created using open banking, or in many cases, broader data sets. However, four submissions also highlighted the importance of ensuring that online journeys are well adapted to people in vulnerable circumstances. Evidence was supplied by an independent expert for example that in research undertaken with people with mental health problems: "*Nearly six in ten respondents [with mental*

*health issues] to our spring 2016 survey (59%) told us that they have taken out credit when unwell, that they would not otherwise have done. Checking consumer understanding with simple recall questions or basic cognitive testing could reduce harm from customers signing up for inappropriate products and services when unwell*." In this, and two other submissions, it was highlighted as a priority that all online journeys designed by providers consider the needs of people with vulnerabilities.

Finally, evidence was submitted about one of the additional risks that open banking can create for vulnerable customers. Open banking payments today can circumvent gambling blocks on debit cards. It is therefore possible for a vulnerable consumer who has blocked gambling on their debit card, to gamble via an open banking payment. Four submissions mentioned this, including two from ASPSPs, one of which reported that: "*We have seen evidence (including from customer complaints) that customers are using open banking to evade card gambling blocks – i.e., those blocks that consumers have themselves requested to prevent them from gambling."*

### Area of Discussion 2: Moving forward on these opportunities

As the evidence above makes clear, there were a large number of proposals put forward in evidence to show how data sharing can create new tools to help identify and support vulnerable consumers. The evidence however was less clear on how to develop these opportunities, to bring them to market or drive adoption of them by vulnerable consumers.

Four submissions were of the view that the open banking ecosystem can already support many of these use cases and most are *"achievable without further development of standards"*. One quote from an ASPSP illustrates this point of view quite clearly: *"Accessing the data is in some respects the easy part, while it can take significantly more time and development to make the necessary changes to use that data in complete consumer journeys - this will require more time and effort to realise."*

Other evidence did however suggest ways in which the Committee could move forward on these opportunities:

- Seven submissions noted that expanding the pool of data would be highly beneficial, making open finance data available, particularly for savings and lending products. In verbal evidence provided at the discussion session on 30 September 2022, one TPP explained that customers cannot understand why some savings accounts are available and some are not. As we have seen above, a number of submissions went further than just open finance data and called for HMRC and other Government data to be made available alongside energy accounts. Two submissions also called for cloud accounting platform data to be made available to support loan decisioning in the SME sector.
- Two submissions noted that the financial viability of many services targeting vulnerable consumers was low. One noted that a service targeting people with mental health problems and another supporting older consumers had withdrawn from the market: *"Promising ideas have in some instances failed to gain traction, not because of a lack of obvious benefit to vulnerable consumers, but due to an inability to effectively monetise the products or services."* There was one suggestion that the FCA should open up sandboxes to help companies develop services and should consider direct support for valuable services.
- Another submission from an independent expert made a strong case that solutions should be based on the lives of those in vulnerable circumstances rather than being identified through evidence gathering in this way. As they noted: *"Our recommendation would be to*

*start this process by undertaking analysis directly with these potential user groups to understand their problems and what they might find useful, and to have this framed from their perspective. An innovation challenge type approach, which frames use cases drawn from real life experiences could be enormously beneficial in shaping the next phase of the development of open banking."*

- Two large ASPSPs urged caution, making the point that not all vulnerable customers are digitally active. One noted: "In order for a customer to use open banking services through a TPP, they are required to sign up to internet banking… As such, open banking users already tend to be digitally capable individuals who use online services to manage their finances. In developing a potential future roadmap, a key risk for the Committee is that in prioritising further support for these customers through digital services it runs the risk of distracting from those with low digital engagement who may have greater need."
- Another ASPSP noted that vulnerable customers can be sceptical about sharing their data and may be reluctant to adopt. They shared: "*Recent experience trialling the use of open banking AIS in the context of affordability checks for vulnerable customers that are being put onto payment plans. [This ASPSP] … has found that these customers are generally suspicious about allowing access to information about their other financial accounts, even if doing so would ultimately save them time and effort. They believe they will be disadvantaged if creditors can see their complete financial status. Customer trust is therefore an important issue when considering how open banking can be used to help vulnerable customers*."

#### *1.18.4.3. Emerging Areas of Alignment*

Overall, there was broad alignment that open banking data sharing can deliver a range of potentially valuable services for customers in vulnerable circumstances. Evidence supplied a long list of interesting and innovative ideas to address a number of issues experienced by vulnerable consumers. Within this, supporting customers with credit applications through data sharing and providing broader insights than those provided by Credit Reference Agencies emerged as the most commonly cited solution, although there were many others.

Although the question was framed as a positive, some did highlight potential risks to vulnerable consumers, with four highlighting the way in which gambling blocks on debit cards can be circumvented by consumers using open banking payments.

There was less alignment on how to move forward, with four large ASPSPs suggesting that there were no gaps or blockers and that the market needed more time.

Others, however, highlighted the vital importance of widening the data pool to include savings and loan accounts, with some going further to full open finance and beyond to government accounts like HMRC and energy companies.

Whilst only put forward in a minority of submissions, some powerful evidence was provided about the need to work with vulnerable consumers to ensure that solutions meet their actual needs and also to consider issues around the financial viability of services.

### 1.18.5. Question 5: Widening Access

***What is the role open banking can play in widening access to financial services products and financial inclusion? Please provide rationale and evidence. More generally, considering ESG, what are the possible use cases and what is needed to support those?***

#### *1.18.5.1. Introduction*

The role that open banking can play in broadening access to financial services received a number of interesting submissions. The question, however, also covered the role that open banking could play in supporting ESG (Environmental, Social and Governance), which is treated separately in this evidence summary, although with some overlaps as we will see.

Three main areas of discussion can therefore be observed in the evidence:

1. **what are the largest opportunities to expand access;**
2. **what are the largest opportunities to support ESG;**
3. **and what is required to support these opportunities.**

We also include evidence that open banking could potentially exacerbate exclusion.

#### *1.18.5.2. Areas of Discussion*

**Area of Discussion 1: What are the key opportunities to improve access?**

A number of opportunities were highlighted in evidence to help improve access to financial services.

**Access to Lending Use Cases**

The use case highlighted most frequently was in the lending space, where the use of open banking data could help to build a fuller picture of a consumer or SME's risk profile and whether a loan would be affordable. This was particularly relevant for consumers on variable or temporary incomes, or those with thin credit files, where open banking data can allow lenders to look at rental payments or evidence of meeting other bill commitments. In total 15 submissions mentioned this opportunity, including expert advisers, ASPSPs, TPPs and platforms.

Some evidence helps to bring this to life: "*5.8 million people have little or no credit history making them 'invisible' to the mainstream credit economy. 2.5 million were narrowly rejected for a credit card or personal loan due to insufficient information (88% of whom are unlikely to default according to Experian). The use of open banking creates a strong S in ESG use case in making financial services more accessible to customers who may otherwise be excluded*." An ASPSP reported that, "*[We] currently use open banking data from other ASPSPs to support credit decisioning for customers who are new to bank borrowing and in some other use cases. We have seen this contribute to our ability to enhance financial inclusion, by simplifying the process for new to bank customers and enhancing their ability to demonstrate credit worthiness through the process*".

Submissions highlighted that the world of credit scoring and credit information is undergoing potential changes. One highlighted the FCA's upcoming Credit Information Market Study and suggested that this could identify an expanded role for open banking. Two submissions suggested that the new FCA Consumer Duty could drive increased use of open banking by lenders.

One submission from an independent expert with expertise in the affordable lending sector highlighted a particularly valuable additional use of open banking in relation to debt consolidation

loans. This submission highlighted that debt consolidation loans are both very common and very beneficial to help consumers escape from a debt spiral. However, the submission detailed significant issues with knowing that funds are actually used to clear down other borrowings. API solutions in this space could help lenders to increase the amount they lend, lend where they may have to decline today and also ensure that debts are properly consolidated.

### Other Proposals

In contrast to the lending use case above, most of the following proposals were put forward by only one or two respondents:

- TPP services for younger consumers, with controls and limits built in. Such services could improve financial literacy and education.
- A 'view only' service for carers was proposed by an ASPSP: "We are, for example, exploring how we could partner in order to provide an open banking-enabled 'view only' option for customers transactions which could be made available to the customer or their carer. For the former, that may replace internet banking where the customer does not want the ability to transact (e.g., because they are worried about getting something wrong), or the latter if the customer wants help, but does not want to give control of their finances away to a third party." (Similar solutions were proposed for vulnerable consumers, See Question 4)
- An ASPSP also suggested that TPPs could provide services with enhanced accessibility for certain types of customers: "Specialist TPPs may be able to present information in a way that is … accessible for specific customers or their carers instead of customers using generic tools (e.g., screen readers). Using open banking, specific customer data could be accessed using a specialist tool, helping customer understanding."
- One response suggested that sweeping services to save or pay bills could expand access.

One independent expert suggested that, with appropriate safeguards, open banking data could be used to create an anonymised data set that policymakers could use to understand consumer issues and pain points in close to real time: "*Anonymised, statistical open banking data supported with innovative AI solutions could be enormously beneficial in providing data and views of spending patterns for particular demographics for policy makers, to enable a true, up-to-date and cohesive picture of aggregated consumer behaviour."*

### Area of Discussion 2: Risk of exacerbating exclusion

It is important to balance the opportunities set out above with a key caveat highlighted in a number of submissions: open banking solutions can only support those that are banked and who also bank digitally. Open banking cannot help consumers who are excluded as a result of lack of digital skills or who are unbanked. As one submission explained, "*Open banking is limited in its capacity to widen access to financial services as it cannot reach the unbanked or not digitally proficient.*" There was unfortunately no data provided on the extent of this in the market, however in a payments submission an ASPSP shared that "*currently c.60% of current account holders are digitally active and regularly use mobile or internet banking",* which gives an indication of the limitations in using open banking as a tool to widen access.

One submission also went further to highlight that the Committee's question did not consider that open banking could exacerbate exclusion or create new forms of exclusion. An independent expert submitted that, *"There is a significant risk that consumers who do not feel comfortable sharing financial data could be excluded from essential financial products and services, or charged unfair prices to access them. To address this, close attention should be paid to outcomes for consumers who do not wish to use open banking, and should ensure that they are treated fairly and are able to access essential financial services."*

Two submissions, one from an ASPSP and one from an expert adviser, both highlighted the risk that the use of open banking could make exclusion worse. It could, in the view of the independent expert, create "*a risk that better use of data will result in some consumers being judged a risk and left unable to access financial services and products*". The submission from the ASPSP suggested that: "*The Committee should be alive to the risk that an increased access to data may lead to an increase in 'cherry picking' by providers where only the lowest risk customers are offered good deals and those with a higher risk score are excluded or priced out from the market*."

### Area of Discussion 3: Role of open banking in ESG

As is made clear, many respondents considered the expansion of credit availability to be consistent with an ESG policy.

Beyond this, six TPPs highlighted the important role that open banking could play in building tools to help consumers and small businesses understand their environmental impact and carbon footprint. One study was quoted which found that, "*Younger consumers are embracing open banking-enabled services that give them greater control over their environmental footprint. This information enables them to look for greener options and eventually switch to those.*" A study of small business decision makers found that, "*68 per cent of small businesses want to operate more sustainably and data is helping make this a real possibility*".

One submission explained the opportunity in this space as follows: "*Open finance could also enable third party applications to obtain financial data that helps individuals and small businesses better understand their carbon footprint and how their actions can help reduce future emissions. Identifying and evaluating transactions related to travel and transportation, utility consumption, purchasing, etc. can enable third party developed services such as carbon and emission calculators."*

There were no dissenting voices around the potential role that open banking / open finance could play in further an ESG agenda.

### Area of Discussion 4: Moving forward on these opportunities

There was less clarity on how the Committee should move forward on these opportunities. A minority expressed the view that open banking already enabled the majority of these use cases and no intervention was required. This viewpoint is most clearly expressed in a submission from an ASPSP that stated, "*We would suggest that such innovation is best left to the market and that in assessing what else may be possible, proper consideration should be given to open banking being only one of a range of potential solutions that may exist."*

Most other submissions tended to highlight a few key changes required to make services in this space more effective and more likely to come to market.

The most common change was the broadening of data sets available, with many calling for an expansion to open finance and some going beyond to "open everything". In the open finance space, there was a call from an ASPSP to focus on opening up savings account and in particular, "*NS&I [National Savings & Investment]... one of the largest providers of savings and 'savings like' products, … which currently does not expose customer data via APIs. We would encourage the committee to review potential new open banking participants such as NS&I to allow customers wider access to financial services products".* Clearly, to support the debt consolidation opportunity highlighted above, lenders would require API access to other lending products.

However, particularly in those championing new environmental tools, expansion beyond open finance was seen as vital, including access to utility accounts and spend level data.

Beyond expanding available data, other suggestions put forward by a smaller number of respondents included:

- Focusing on building trust in open banking. To be an effective tool to broaden access, consumers must trust open banking. This is addressed in the Ecosystem Sprint, Question 7.
- One submission from a TPP shared detailed information on some of the challenges of using open banking data for loan decisioning. Two areas of enhancement were set out in detail. The first was for a greater degree of consistency in the way data was shared and additional transaction level detail. More significantly for this TPP, they needed a regulatory change which would allow them to use open banking data in ways beyond the PSD2 consent, to enhance and improve credit risk models.

#### *1.18.5.3. Emerging Areas of Alignment*

There was broad alignment that open banking could play a role in widening access to financial services, particularly around access to credit. There was persuasive evidence that this impact was already being seen and there was potential to go further.

However, a minority of views urged caution that open banking could also be used to exacerbate exclusion, outcomes which would need to be carefully monitored in the view of some submissions.

There was less alignment on what activities were required to move the market forward and to accelerate services focused on financial inclusion. Some suggested that most valuable use cases were supported today and that no action was required. However, a clear majority of responses called for an expansion of the data sharing ecosystem, bringing in open finance accounts (savings and loans in particular) and going beyond to incorporate access to utility accounts to create more powerful, insightful environmental tools for people and small businesses.

### 1.18.6. Question 6: Critical capabilities and functions

***Consider the critical capabilities and functions the ecosystem and/or the Future Entity would need to support further data sharing propositions beyond open banking (e.g., considering future open finance framework)***

### *1.18.6.1. Introduction*

A range of responses were received in answer to this question, some focusing on shorter term issues with others focusing on longer term challenges that need to be addressed to ensure the ecosystem is robust enough to support an expansion of data sharing propositions beyond open banking

### *1.18.6.2. Areas of Discussion*

**Area of Discussion 1: Focus needs to be on improving API performance**

Seven TPPs specifically called out the quality and performance of the APIs as a current issue for open banking data sharing. Many felt that the need to review and improve current performance was of the utmost importance before the development of new capabilities. In evidence submitted to this Sprint no ASPSP commented on API performance and availability, but in the Payments Sprint they did submit evidence showing performance was at least as good as direct channels. In the Sprint discussion meeting one ASPSP referenced the improvement in API performance that had been achieved and this was demonstrated in the OBIE-reported MI.

A number of TPPs stated that the performance of smaller banks and credit card companies was worse than large institutions, and one TPP stated that a particular bank had a technical error rate of 50%. Another TPP stated that there is *"not even a single day which goes without downtime"*.

**Area of Discussion 2: Longer term changes to support wider data sharing**

Two ASPSPs challenged whether the current model for Trust and Security services was suitable in the longer term. One TPP noted that Trust and Security services could be delivered in a distributed model but was not advocating for change and thought that the current centralised model may offer synergies as only one entity needs to check FCA permissions. Five ASPSPs explicitly called for a more balanced funding system for the Future Entity compared to the current model under the CMA Order.

### *1.18.6.3. Emerging Areas of Alignment*

**Monitoring and enforcement**

A number of responses from ASPSPs, TPPs and expert advisers referenced the need for a wider and more comprehensive monitoring and enforcement regime to ensure all market participants operate on the same standards. One TPP cited the variation in performance was a market failure that warrants regulatory intervention. However, there was no consensus on the objectives being sought or the mechanism to achieve that. TPPs wanted more consistency across data providers, independent observers wanted to ensure an open market, and ASPSPs wanted a common oversight regime. A number of TPPs also highlighted the importance of ASPSPs responding proactively when issues arise. One TPP shared data on tickets that they had raised through the OBIE Service Desk, which identified that one ASPSP was taking 175 days to resolve issues, with many others taking over 50 days.

**Regulation and Incentives**

A number of respondents referenced the expansion of open banking data sharing to include information of different types of accounts such as savings, credit cards, mortgages investments, etc.

Expert advisers, ASPSPs and TPPs noted that there was no incentive for data holders to invest in the capabilities to share further data sets with third parties and so regulatory intervention will be required to expand the markets. In the discussion, one ASPSP cautioned that the investment was very large for PSD2 so this would have to be a very considered decision, but market expansion was unlikely to happen without it.

#### *1.18.6.4. Other observations*

An independent expert identified that it may be necessary to introduce additional protections as data can be shared with companies outside of the FCA perimeter. However, the challenges of developing and overseeing any such protections was clearly noted. This is further discussed in the Ecosystem Sprint, Question 9 (Onward Sharing).

### 1.18.7. Question 7: Standards and Guidance

***What additional standards or guidance would be needed to support use cases discussed above? Please provide rationale and evidence.***

There were a range of short-term and longer term perspectives in the responses received.

#### *1.18.7.1. Areas of Discussion*

**Area of Discussion 1: Enhancing the standard**

It was felt from a number of contributors that additional standards and guidance may be necessary to address some short-term issues. Several TPPs and expert advisers felt that all ASPSPs should adopt the Open Banking Standard. One TPP highlighted a new market entrant that has signed up millions of customers but does not plan to make available open banking APIs until 2023. Several TPPs highlighted that a number of fields in the open banking standard are optional, leading to inconsistent use, and the market would benefit from a more consistent approach if optional fields became mandatory. An ASPSP identified the need to enhance open banking standards by enabling Confirmation of Payee and CRM Warnings. However, the ambition and priority to enhance different elements of the existing standards was not universal.

**Area of Divergence 2: Managing consent and Processing of Data**

One independent expert identified that a robust data ethics framework is required to support the expansion of data sharing propositions beyond open banking. A second independent expert queried whether additional protections are needed as onward sharing of data can take place to companies beyond the FCA regulatory perimeter. A number of ASPSPs questioned on what basis data was being shared and whether it would involve different operational processes (e.g., different authentications) if the same firm was supplying PSD2 and non-PSD2 data.

A TPP noted that, as data sharing becomes more embedded, the more difficult it is for the consumer to keep track of where they have given permission and how long when they are dealing with multiple different TPPs and data sharing agreements. Another TPP noted that the requirements for consent were clear, it is the role of the TPP to manage consent with the customer. There is more discussion of the issues of Consent in the Ecosystem Sprint, in response to Question 8 (Customer understanding and awareness).

#### *1.18.7.2. Other observations*

Respondents also identified a number of other areas where standards and guidance would be beneficial, but there was limited consistency as to whether they should be advisory or mandatory. The areas suggested included:

- Consumer guidelines
- Relationship with the NPA
- Pending and booked transactions
- Merchant categorisation
- Identity
- Cyber security
- Data misuse
- Use cases for underserved customers
- Illegal lending
- Data on closed accounts
- Fraud warnings and CoP.

### 1.18.8. Question 8: Multilateral agreements

***What areas would MLAs covering services beyond the Order and existing regulations need to cover in order to facilitate continued development of data sharing under open banking in a safe and efficient manner? Please provide rationale and evidence.***

#### *1.18.8.1. Areas of Discussion*

**Area of Discussion 1: Role of regulation**

Three different approaches were identified from submissions and the sprint discussion:

**Regulatory-led**

It was noted by banks, TPPs and expert advisers that there were limited incentives for data holders to make their data available to third parties. Therefore, it was likely that some form of compulsion would be required to open up new data sharing markets. Several TPPs supported the notion of customers having a right to access their data. A number of ASPSPs cautioned about being overly prescriptive with regulation and in the Sprint Discussion held on 30 September 2022 referenced that they had built end points for open banking that had not been used. One TPP questioned whether lack of take-up was due to there not being a platform stable enough for them to develop propositions (where all banks are at suitable levels of performance).

**Market-led**

A market-led approach to innovation was cited as optimal by a number of respondents including platforms and ASPSPs. However, concerns were raised in the submissions and in the discussions on this topic: an expert adviser cautioned against market fragmentation; an ASPSP cited that the voluntary approach had not resulted in the adoption and use of the Extended Customer Attributes standard; and a TPP stated that unrealistic commercial expectations was one of the reasons why non-sweeping VRPs had stalled. In the discussion, another TPP referenced the challenges to a market-led approach based on the roll out of open banking services in the US and advocated for a more regulatory driven approach for the UK.

**Mixed approach**

TPPs and ASPSPs suggested that some combination of regulation and market-led approaches would be an optimal outcome. However, there were different views around the scope of different areas. Inclusion of liability and disputes was generally agreed upon, whereas there was a difference of views as to whether commercials should be included. Some TPPs advocated a price cap for commercial VRPs, whereas others felt that access to VRPs should be free. An ASPSP expressed a concern that they are not able to even recover costs for providing access to data via APIs so further opening of data sets would be challenging.

**Area of Discussion 2: Bilaterals or multilaterals**

A platform advocated for bilaterals as the most appropriate next step for the development of open banking, but an ASPSP highlighted that development of multilaterals would be difficult given the large number of participant firms in the open banking ecosystem. However, there was a larger number of TPPs and trade associations which felt that bilaterals were not the right approach and some stated they would be particularly difficult for smaller TPPs which would not have the resources to negotiate with multiple banks. One ASPSP highlighted the importance of ensuring competition law was considered when developing any MLAs.

### 1.18.9. Additional Commentary:

***Please add additional commentary if there are topics which respondents feel would warrant consideration by the Committee. Please provide rationale and evidence.***

Twenty-five respondents did not provide any additional comments.

Two respondents noted that identification of relevant gaps that were impeding the scope for extending open banking for SME finance had not been included in the Committee's questions. They felt that this merited consideration. Broadly their position was that, while there is a reasonable level of current available data sources, improving the accuracy of these would be beneficial.

Other respondents noted in relation to fraud that broader range of cross-industry actors that can and must act to prevent fraud, of which data sharing plays a part in the solution, alongside other measures.

One TPP expressed a desire to consider the requirement to extend beyond the parameters of open banking today. It argued that is imperative that we progress the work of open banking, open finance and smart data in an organised, efficient and swift way and that failure to do so risks the UK risks losing its global leadership on this important topic to other nations that have co-ordinated efforts from the outset.

One trade association suggested that unlocking and integrating other data sets from a broad range of markets and the public sector would be of significant potential benefit for customers.

Two respondents stated the importance of cost / benefit analysis to ensure any requests on market participants are proportionate. They pointed to evidence of significant investment in solutions that were ultimately not adopted or did not achieve the outcome intended. Given the costs of implementing data sharing, they argued that further development should be commercially-led providing incentives across the market, with any regulatory intervention limited to instances where there is clear evidence of market failure and customer detriment.

## 1.19. First Ecosystem Strategy Sprint

### 1.19.1. Question 1: Gaps in Journeys

***Are there any gaps in current guidance and standards to ensure efficient and safe customer journeys and support broader use cases? If so, what is missing and what needs to be changed?***

#### *1.19.1.1. Areas of Discussion*

A very wide range of issues were identified in responses to this question, topics on which there were multiple responses are highlighted below.

**Area of Discussion 1: Fraud and high value payments.**

Fraud and the ability to reliably facilitate high-value open banking payments was a key issue highlighted in the ecosystem sprint. (It was also a key issued raised in the payments sprint). Two ASPSPs provided new evidence around the level of open banking fraud, and this is presented below:

***Figure 5: ASPSP 1 Fraud evidence***

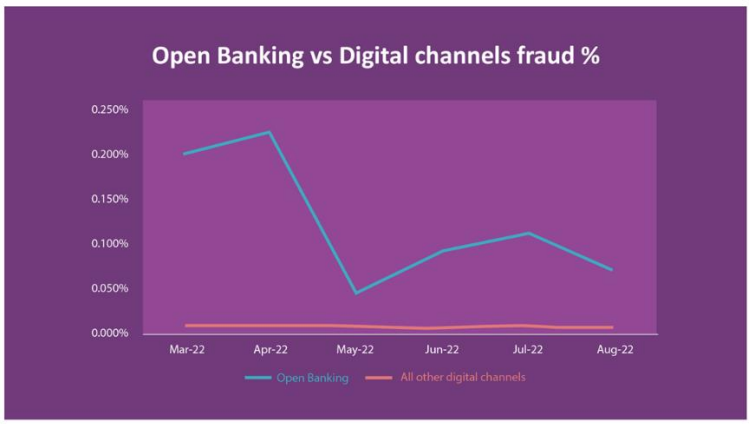



***Figure 6: ASPSP 2 Fraud Evidence***


The first graph shows that for one ASPSP over a six-month period there is 15x more fraud in open banking payments compared to other digital channels. The second graph shows the level of attempted fraud in open banking channels is twice that of other channels for another ASPSP. During the sprint discussion session held on 7 September 2022 a number of TPPs were keen to understand more behind the drivers of this fraud, such as whether it was particular propositions that were driving the increase in fraud and the nature of the fraud vectors.

The link between the blocking of high-value transactions as a consequence of actions to reduce the level of open banking fraud was also highlighted during the Payments Sprint and five responses indicated that the lack of ability to consistently undertake high-value open banking payments was undermining the ecosystem. These responses came from TPPs and a trade association. No ASPSP identified high-value payments as an issue for the ecosystem.

### Area of Discussion 2: User experience.

A number of respondents cited in their responses that there was a need to improve the user experience in open banking, and a particular issue was related to instances when the customer would have to undertake multiple authentications using SCA. Nine respondents noted that advice and guidance were needed to address this issue. Three platforms, two trade associations and four TPPs raised this as an area of concern and again no ASPSP identified this as an issue.

An independent expert identified a range of concerns around existing customer experiences, particularly around consistency in communications, and ensuring dashboards are an effective tool to inform consumers and SMEs what open banking permissions they have granted.

### Area of Discussion 3: Payment status.

Payment status and a way for TPPs and end customers to understand with confidence whether a payment was successful or not was highlighted as an area that was restricting the potential for open banking payments and this was raised by part of the ecosystem, with four trade associations and three TPPs identifying this as an area that was restraining the growth of open banking payments. Again, no ASPSP raised this as an area of concern. This was also extensively reviewed as part of the Payments Sprint, see Question 4 (Functional Capabilities).

### Area of Discussion 4: Expansion of VRPs

Many, but not all of the respondents who raised payment status as an issue also highlighted the need to expand either the definition of sweeping, or allow VRPs to be used for a broader range of use cases. Four trade associations, two TPPs, but no ASPSPs raised this point. The independent expert expressed some concerns around the maturity of the use of VRPs for sweeping and whether they delivered the outcomes expected by the CMA.

### Area of Discussion 5: Capability expansion and standard enhancements

In addition to expanding the payment capabilities to facilitate clarity on payment certainty and expansion of VRP capability a range of other enhancements were recommended, this includes:

- Inclusion of a frequency parameter in VRPs (independent expert)
- Expansion of the data sets available to include other products (independent expert, three trade associations, two TPPs)
- More consistency and classification in existing data sets: *"AIS data is inherently messy" - TPP*

Standards and guidance were seen as a way to achieve more consistency in error messages, which would lead to better experiences for customers as the TPP will be better able to manage the customer's expectations. Two trade associations and one TPP raised this point in response to this question.

#### *1.19.1.2. Emerging Areas of Alignment*

**Wider application of Standards**

Across the ecosystem respondents called for a wider and more consistent application of the UK Open Banking Standards to drive more consistency across the ecosystem in terms of technical standards and customer experience. Two trade associations, two TPPs and two ASPSPs called for the UK Open Banking Standard to be applied more consistently across the ecosystem, some called for application to all banks, not just the CMA9 banks, and others also called for TPPs to apply the Standard and there to be a monitoring regime for all participants.

**Need for an agreed disputes and liability framework**

Again, participants from across the ecosystem called for the development of a consistent framework for liability and customer disputes. Four ASPSPs and a trade association cited lack of an agreed framework as a gap in response to question 1. However, there was no detail provided regarding how the dispute framework might work in practice or where different liabilities should reside.

**Incorporate appropriate messaging into open banking journeys**

Three ASPSPs called for an update of the standards to enable CRM warnings and CoP to be deployed in open banking journeys, one trade association which includes TPPs and banks in their membership also supported this proposal. This did not appear to be a topic of disagreement during the Sprint discussions, although unnecessary friction in open banking journeys was a broader concern raised by TPPs in discussions and submissions.

**Improved sharing of data between participants**

Improving data sharing between parties was another area where participants seemed to find common ground, with an ASPSP, a TPP and a trade association specifically supporting increased data sharing. However, there were differences in regard to the detail and the mechanism for this data sharing such as using TRIs, sharing participant details in the consent flow rather than via software statements, or the bank providing details to the TPP to help prevent fraud.

### 1.19.2. Question 2: API Performance

***Is there a need to improve API availability and performance? What is the evidence and how could it be addressed?***

#### *1.19.2.1. Areas of Discussion*

**Area of Discussion 1: The need for improved performance.**

Four ASPSPs cited that API performance matched that of their direct digital channels and so further improvement was not necessary. However, two platforms, six trade associations and five TPPs stated that there was a need for improvement in API performance and that there was significant variance across all banks (large and small) across the ecosystem. Respondents provided new evidence by way of examples of poor performance, for example:

> *"Open banking bank feed reliability remains one of the most important issues to address. It continues to present the biggest obstacle to realising the full potential benefits intended from open banking… connections at one banking institution fail every time we try to retrieve transactions… in 2022 the highest average time to resolve issues so far was 175 days."*
> *– TPP*

> *"Convergence rates drop dramatically (by over 45% over a seven-day period, in one case) when ASPSPs experience unscheduled API downtime." – trade association*

> *"Drop-off rates vary between 23% and 53% for [CMA9 banks] and between 11% and 85% [for others]" – platform quoting a TPP.*

If open banking payments were to compete with cards both ASPSPs and TPPs noted that the availability levels may need to increase to the level experienced by cards and so increase from 99.5% availability to 99.999% availability. Sprint discussions highlighted that investment would be needed to achieve this level of change in availability.

#### *1.19.2.2. Emerging Areas of Alignment*

**Transparency and reporting of performance.**

One proposed method to improve API performance was to increase the reporting and visibility of API performance and potentially other performance metrics such as response time and completions rates. Improved reporting and visibility of performance statistics was proposed by one ASPSP, four TPPs, and six trade associations and an expert adviser. However, there was no clear agreement on the mechanism to achieve this increased level of reporting.

### 1.19.3. Questions 3 and 4: Multilateral agreements

***What areas would MLAs and updated Standards covering services beyond the Order and existing regulations need to cover to facilitate continued development of open banking in a safe and efficient manner? Why?***

***Are there blockers in developing MLAs? Please provide rationale and evidence. Who should be responsible for administering, ensuring compliance with, and taking forward future changes to such agreements?***

#### *1.19.3.1. Areas of Discussion*

**Area of Discussion 1: Need for MLAs**

The submissions to the SWG secretariat and the discussions at the Sprint Discussion meeting highlighted a broad range of opinions regarding the need for MLAs. An ASPSP and a platform both indicated that whilst MLAs had benefits it would be more appropriate at the moment to let the market develop with bilateral agreements. However, a larger population of respondents indicated that MLAs would benefit the development of the ecosystem. Some TPPs cited concerns that bilaterals could provide barriers to entry, smaller TPPs may not have the resources to negotiate contracts with multiple banks, as it would also take a significant amount of time to negotiate agreements with all the banks.

**Area of Discussion 2: Elements of MLAs**

Six respondents indicated that they thought any multilateral agreement should include clarity regarding **disputes and liability**. This view was held across the ecosystem with two ASPSPs, two platforms, and two trade associations stating this view.

One ASPSP, two TPPs and one trade association stated that MLAs would be a useful mechanism to ensure **operational performance** of the open banking end points.

Five respondents recommended that **commercial terms** should be included in MLAs, but the challenge of determining commercial terms whilst not contravening competition law was referenced in submissions and in the Sprint Discussion meetings. Furthermore, one TPP submitted a view that the development of commercial APIs for any open banking payment capability would undermine the development of the open banking payments market. The challenge of developing a commercial framework that was viable for all members of the ecosystem was noted in both Sprint Discussions and in submissions:

> *"The biggest blocker is the current lack of a viable commercial model for open banking."* – *trade association*
>
> *"The biggest 'blocker' is likely the level of complication in those agreements and agreeing a framework which works for everyone, including on challenging items such as commercial and liability model."* – ASPSP

**Area of Discussion 3: Need for regulatory intervention**

There was a broad range of views regarding how MLAs would be brought to market ranging from letting market forces lead to the development through to direct regulatory or statutory intervention. The perspectives submitted as evidence are highlighted below:

Two ASPSPs, one platform, two trade associations and one TPP indicated that they felt that development of MLAs was purely a **commercial** matter. One of the ASPSPs provided more detail indicating that they thought participation in an MLA was purely voluntary, however it was entirely possible that signing up to an MLA would have binding obligations on the firm (e.g., conformance and performance SLAs). This is how schemes operate in the payments space.

A number of firms indicated that they felt some form of targeted interventions might be necessary, with the regulatory intervention being highly targeted only in areas where the market to agree is unable to agree terms. Whilst details were not specific, two payment associations and two TPPs indicated an expectation of this latter approach.

Several TPPs in a trade association response and two TPPs, and one trade association specified the need for **regulatory intervention** to open access to new markets, both new structured data sets and to support the development of the A2ART market. Expert advisers also expressed the benefits of a regulatory driven approach. A regulatory driven approach has supported the development of successful data sharing in other geographies and would ensure that there was appropriate protection for consumers. One independent expert referenced a quote from a UK consumer body that stated that:

> *"[The] preference would be for the regulator(s) to establish a scheme for open banking payments that is open to scrutiny and challenge which reflects the needs of end users, including consumers."*

### 1.19.4. Question 5: Disputes

***Identify current gaps and identify what may be needed to put in place effective dispute management, redress and resolution mechanisms and processes across ecosystem participants, e.g., between ASPSPs and TPPs, between end-users and ASPSPs and TPPs?***

#### *1.19.4.1. Areas of Discussion*

**Area of Discussion 1: Gaps in current dispute resolution processes**

There were differing views expressed in response to this question. The majority of TPPs stated that there had been a very low level of disputes between ASPSPs and TPPs to date, with little evidence of disputes and low propensity for fraud. They did not see any existing gaps in the current dispute processes, with the small volume of previous disputes having been handled effectively and efficiently. Some TPPs indicated that this was a consequence of the clear obligations under PSD2 where banks bear liability for execution of payments under PSD2 and consumers have a right to redress from their bank if there is an unauthorised or defective payment. Consequently, there are very limited payment disputes concerning who is liable for a payment.

While ASPSPs have a legal right of action, and right of recourse to a PISP if the reason for the defective payment was due to the PISP, this was extremely rare and these respondents felt that disputes were best handled bilaterally by participants on an ad-hoc basis. However, one TPP stated that the management of inter-firm interactions to resolve the small number of issues arising did not appear to be either timely or efficient.

All respondents agreed with the assessment that there had been very few disputes to date, and many noted that the existing Dispute Management System in place is almost entirely unused by ecosystem participants and is likely to be decommissioned as a result. However, the majority of respondents believe that the evolution and wider adoption of open banking payments will necessitate development of a more effective and robust dispute resolution mechanism.

These respondents argue that A2ART payments are more prone to disputes and increasingly there will be a need for a dispute resolution mechanism that can operate efficiently at scale as this use case becomes more prevalent. Developing trust in A2ART payments will therefore depend on a significant improvement the existing disputes process. Many respondents noted the criticality of this capability in other existing payment networks. Some respondents, primarily ASPSPs, also view the emergence of non-Order functionality such as non-sweeping VRPs as a driver for improved dispute resolution capability, as clear arrangements will be needed to manage disputes and liability under agreed contractual terms between TPPs and banks. One bank considered that possible changes to APP fraud reimbursement being considered by the PSR would require liabilities to be shared between both parties in the payment chain, which could require more complex dispute resolution mechanisms.

ASPSPs generally identified a requirement to ensure customers receive equivalent protections to alternative payment methods as a future driver for significant further development of the disputes model. One ASPSP stated that this should be undertaken prior to the growth of A2ART payments to ensure customers are not left unprotected. Expert advisers also noted that the potential impacts of the new Consumer Duty on firms might have an impact on future requirements.

Most respondents who identified a need for development of better dispute resolution mechanisms for payments did not see a similar need in relation to data. However, expert advisers took an alternative view. They presented evidence that there were existing gaps in several areas, notably:

- There is no mechanism for identifying potential risks to end users and allocating responsibilities for mitigating these.
- There was no existing requirement on participants to escalate or report significant operational events or data breaches to other parties involved.
- There was ambiguity as to how redress would be provided for in the event of a data breach within or across a regulatory perimeter.
- GDPR rights and access to Financial Ombudsman Services (FOS) and the FCA regulatory perimeter do not apply to SME / Corporate data.

There were divergent views on the role that FOS should play in settling customer disputes. Some respondents considered that it would be more efficient to have an internal arbitration framework, but an independent expert viewed FOS as a having more independence and credibility

### Area of Discussion 2: New dispute mechanisms to address the gap

Three possible solutions were identified by respondents, who had identified a material existing gap.

#### *Process Standardisation*

Several TPPs, one ASPSP and a trade association believed that a standardised process protocol, building on dispute and liability frameworks, could supplement existing regulatory payment dispute rules. The identified gap was how legal requirements can be applied in a consistent manner to new open banking payments use cases. What is not in place is a way to standardise/ operationalise how 'payment disputes' between banks and PISPs are managed. These responses noted that the FCA Approach Document referred to "PSP agreed arrangements for the settlement of such liabilities between themselves".

It was suggested that this might comprise a tool for communication of agreed approach datasets as well as a process definition defining liability, SLAs/timelines for disputes etc. The ASPSP also indicated the need for a challenge and arbitration process to resolve disputes.

#### *Scheme Rules*

Most of the ASPSPs considered that the introduction of multilateral contracts governing inter-party liabilities would require a well-defined arbitration process, underpinning where the contracts provide contractual legal obligations and process for redress. A commonly expressed view was that the disputes processes and the associated liability model should look to replicate the successful logic and features of the process established by the card schemes.

Introducing any new complaints handling procedures comes with significant operational overheads for PSPs and merchants. Where possible open banking payments dispute resolution mechanisms should seek to build on current regulatory requirements and best practice, rather than introduce new obligations. Other bank respondents were more cautious, agreeing in principle that mechanisms will be needed, but they must be targeted and applied with a clear understanding that they will increase costs on providers and therefore costs on end users – undermining one of the key competitive advantages of PIS payments versus legacy products such as cards.

*Regulatory Change*

Two large ASPSPs argued that it may be more appropriate to define a role for the PISP to manage open banking disputes on a day-to-day basis. This was particularly the case for disputes relating to authorised payments, for example disputed purchases, delivery of goods, quality of goods or services and refunds, where the PISP had responsibility for the role of the merchant, and the services provided.

An independent expert noted that Australian legislation provides clarity on the obligations of data holder and data recipient which provides a firm foundation for a data sharing ecosystem, "*The legal foundations of Australia's CDR include a multilateral contract established by statute. Also, the CCA legislation (s56GC) establishes a legal liability structure between participants, under which data holders and data recipients are protected from legal liability in complying with the CCA and the CDR Rules (including the Standards).*"

### *1.19.4.2. Emerging Areas of Alignment*

Given the wide variety of views as to the existence of a gap at all and then how to bridge it, there were few areas of alignment. However, several respondents did indicate that the Credit Payment Recovery service for Faster Payments operated by Pay.UK should be developed to cater for future retail use cases.

The majority of respondents suggested that efficiencies may be drawn from an arbitration framework for dispute resolution, managed by a central body, rather than reliance upon Payment Services 2017 regulations or satisfaction of unresolved disputes through FOS / court action, but this was not a universal view.

### 1.19.5. Question 6: Crisis Management Plan

***Discuss and consider the development of a crisis management strategy and plan.***

#### *1.19.5.1. Areas of Discussion*

The predominant view across most respondents is that central crisis management planning is unnecessary and would represent duplication of existing efforts. It was commonly noted that individual providers will each have their own plans in place, with accompanying scenario planning which is regularly tested. It was extensively noted that firms have similar arrangement in place, subject to scrutiny by regulators.

Some TPPs expressed concern that centralising this activity, could lead to duplication and disincentivise participants from taking individual responsibility for these critical areas.

One TPP suggested that crisis management strategies and plans could form part of bilateral or multilateral framework agreements, but should not be a prerequisite for the provision of open banking services.

An independent expert provided insights during the Discussion Session on 7 September 2022 relating to a large data breach from a large telco party in an international market, which is due to join their data sharing ecosystem. This has encouraged the development of a crisis plan. A particular consideration would be given to enable participants to be suspended or removed from the framework if their continued participation would harm other participants or the framework itself.

A trade association and an independent expert suggested that open banking is not currently prepared for a crisis, such as a major data breach. Their view was that this potentially means that open banking may not meet the level operational resilience required by the Bank of England. Key concerns include an absence of overall ecosystem plans and responsibilities, lack of a notification protocol and clear definition of responsibilities of different parties including unregulated TSPs. The expert suggested that as a result of these obvious deficiencies any response to an incident was likely to be delayed and fragmented. These respondents identified the need for a facilitator function to coordinate responses, in the event of an ecosystem crisis

An independent expert and a platform said that end-users need confidence that they would be safeguarded. Systems need to be in place to respond to a crisis, to avert the risk of credibility within the broader infrastructure. It is important that these capabilities are tested so that there is confidence in the proposed response to disruptive situations. The expert further argued for a self-managed but centrally understood incident response capability with a central tool or process to record, evaluate, escalate and resolve issues as quickly as possible after they occur to minimise service disruption

Several ASPSPs and a trade association suggested that more focus was required to mitigate the concentration risk of shared infrastructure. The growth of open banking will increase the systemic importance on the shared infrastructure. These respondents stated that it is not clear how a prolonged outage of the Open Banking Directory, or a security breach would be handled. They referred to previous Directory outages, which if they had not been resolved may have impacted both open banking and CoP services. If that had happened, it was not clear how this would have been centrally managed and communicated to parties and consumers.

#### *1.19.5.2. Emerging Areas of Alignment*

There was considerable divergence in views presented, with the predominant view that participants are suitably prepared and little appetite for greater central co-ordination. Wider industry coordination would only be required, and an appropriate industry body should be given this remit, if it is evident that particular risks cannot be mitigated through ordinary industry cooperation.

### 1.19.6. Question 7: Trust

***Is something needed to further strengthen consumers and other end users' trust in open banking? Should tools such as trust marks be considered or not? Please provide rationale and evidence.***

#### *1.19.6.1. Introduction*

The question of trust in open banking is a complex one and there were a wide range of views and evidence presented. Some responses differentiated between data and payments, others focused on one or the other and some made generic comments across both data and payments. This has been recorded in the text.

#### *1.19.6.2. Areas of Discussion*

**Area of Discussion 1: Is there a trust gap?**

Not all respondents directly addressed this question, but those that did presented quite significantly differing perspectives.

Four responses, from ASPSPs, suggested that trust was not an issue, or certainly not the most pressing issue facing open banking. As one response noted, "*We are not aware of evidence that there is a lack of trust in open banking amongst users.*" All these submissions cited the current growth in users as evidence that there did not appear to be a fundamental trust issue with open banking payments or data sharing. One of these responses clarified that in their view the biggest issue holding back open banking payments was not trust but awareness.

One independent expert suggested that there were trust issues amongst SMEs, but one TPP cited a research study which had found that "*A very large proportion (67%) of senior SME stakeholders are willing to share finance data… This figure rises significantly to 90% for larger SMEs, with ten or more employees.*"

A TPP also provided evidence that suggested that UK consumers' concerns about data sharing had started to reduce: *"A Deloitte study has shown that when it comes to data privacy, UK consumers are becoming less worried about the use of their data, with the percentage of people reporting to be 'very concerned' about their data usage dropping from 47% in 2018 to 24% in 2021."* This TPP also quoted research by McKinsey which pointed to other factors being more important in determining whether consumers are happy to share their data. This research found that *"…willingness to share data doubles when customers find an appealing product or service enabled by their data or understand the value it might bring them."*

Two pieces of evidence were provided which offered a more nuanced picture, acknowledging that trust was an issue, but not the only one holding back adoption. One of these focused on payments, one on data, but they came to similar conclusions.

A TPP provided evidence from users of open banking payments. This research explored what changes would make people more active users. The top four responses were:

1. **Less screens to click through – 24.88%**
2. **Reassurances about security – 22.68%**
3. **More visibility about the length of the process – 21.22%**
4. **Clearer instructions before I initiate a payment – 15.37%**

Only the second of these factors has a connection to trust, leading this TPP to conclude that trust played a role, but other factors were also important.

The final piece of evidence was a published piece of research by Frontier Economics which explored the Economic Impact of Trust in Data Ecosystems[7]. This study drew the conclusion that if levels or trust are enhanced, we do see corresponding willingness to share data also increase, however: *"These aggregate results show that even large increases in trust will only correspond to moderate impacts on willingness to share data overall. This serves to emphasise that there are many factors, alongside trust, which cause data sharing to be lower than optimum. Increasing trust without addressing these other factors is unlikely to be sufficient."*

### Area of Discussion 2: Opportunities to enhance trust

Whilst there was a strong focus on trust marks in responses, there were other recommendations put forward to enhance levels of trust.

Eight responses suggested that the consistency, reliability and standardisation of the open banking experience was key to driving trust. As one submission stated: *"Standardisation, consistency, and reliability remove hurdles to the end user completing their first experience, which is the first step in building trust."* These responses came from across the ecosystem including two ASPSPs, two platforms and four TPPs.

Five responses proposed that work to drive awareness would help build trust levels. This was supported by three ASPSPs and two TPPs. Some further suggested that awareness-building should be linked to official communications by Government to underline the safety of open banking. As an example, one submission concluded that: *"Awareness campaigns and information on how to identify safe and trusted applications would be beneficial."*

Four submissions focused on the use of negative or discouraging language by ASPSPs and suggested that more positive language would build trust.

Four submissions focused on language (two for payments, two for data), calling for more intuitive and consistent naming to be used. One platform described the low levels of success of a P2P payments service and attributed part of the failure to the lack of consistent naming and description.

[7] See here

One submission suggested that the best way to build trust in payments was to encourage first use. This TPP called for a "hero" use case (such as utilities) which could be offered with an incentive to encourage new users.

### Area of Discussion 3: Role of trust marks

Unsurprisingly, the role of trust marks received significant weight in responses, as it was specifically cited in the question by the Committee.

There was a spectrum of responses from strong advocates to strong opponents, however, in simple terms, we recorded nine responses in favour of a trust mark and nine opposed. Amongst proponents, were two expert advisers, two platforms, two ASPSPs and three TPPs. Opponents were more skewed to ASPSPs (with four opposed), but also included four TPPs.

There was some interesting evidence submitted.

One independent expert highlighted that the data sharing ecosystem in Australia has adopted a trust mark. Evidence was unclear on the role that it had played, and comparisons with the UK are hard, but it appeared to have been helpful in promoting trust.

A TPP supplied evidence from a recent research study (also quoted above) which found that: *"A 'trust mark' scheme would therefore have a moderate, but positive impact on building trust with SMEs. For example, senior SME decision makers reported a 9% increase in the likelihood that they would "maybe" share financial data to a lender with government endorsed 'trust mark', and a 4% increase for those who would "definitely" share their data."*

Both evidence points suggest that a trust mark could have a mildly positive effect. However. other respondents quote work undertaken by OBIE which investigated the role of trust marks in detail and concluded that there wasn't a sufficiently strong case to proceed with the development of a trust mark within the scope of the CMA Order.

### Area of Discussion 4: Trust mark considerations

A number of respondents highlighted important aspects of trust marks which would need to be considered if work was to move forward.

The most commonly cited consideration was that any trust mark must "stand for something" and point to some tangible protection. Four respondents raised this issue.

Other considerations raised in evidence included:

1. **The question of who certifies and administers any trust mark.**
2. **The need to promote any trust mark, raising questions of how costs are allocated across the ecosystem.**
3. **How to prevent fraudsters spoofing a trust mark in order to give false reassurance to customers.**

The final consideration would be whether the trust mark covered data or payments or both. Most responses were silent on this point, but overall there appeared to be a stronger case for a trust mark on payments.

#### *1.19.6.3. Emerging Areas of Alignment*

This was an area with quite significantly divergent views. If work is to proceed in this area it would therefore need to address the real issues and concerns raised, including the fundamental question of whether a trust mark is needed and how significant a trust issue there is with open banking.

The one area of broad agreement was that trust is created through a complex mix of factors, including consistency, reliability and language and that building trust would require much broader work than simply the creation of a trust mark.

### 1.19.7. Question 8: Consumer understanding and awareness

***Are further tools or guidance needed (or not) to increase consumer understanding and awareness, including in considering consent management? Please provide rationale and evidence***

#### *1.19.7.1. Introduction*

Written evidence included only limited data on the extent of consumer understanding and awareness today, which makes it challenging to define exactly the nature of the gap in this space.

#### *1.19.7.2. Areas of Discussion*

**Area of Discussion 1: Is there a gap?**

The first question to consider in reviewing the evidence is the extent of a gap in the space of consumer understanding, awareness, and ability to manage consents. There was limited empirical evidence provided, although a number of viewpoints were put forward.

One independent expert quoted research conducted by BEIS which found that: *"TPPs do not always provide clear and transparent information on their key Terms and Conditions of the service and Privacy Notice to consumers, so the implications of giving consent may not be well understood. There is a tendency towards a lack of transparency e.g., the consumer must scroll to the bottom of the page and agree without reading, or at best skimming the text, during which they may not have paid attention to the Privacy Notice."* This suggests that consumer comprehension of what they are consenting to is likely to be quite limited.

Other submissions, inferred from adoption rates that consumer general understanding and awareness must be high*: "For example, c75% of new to bank loan applicants voluntarily choose to use open banking to share their transaction history with [the bank] rather than use alternatives (such as PDF statement upload). Therefore, we do not see a need for additional awareness activities."*

Another submission suggested that "*for the current, supported uses cases in the Order, we've not seen evidence that further tools are necessary*".

However, looking across all the evidence a number of submissions put forward areas of focus or recommendations on activities that should be progressed in this space, suggesting that there is a gap that needs to be addressed. In total, 12 submissions made recommendations for activities that should be considered by the Committee.

A number of submissions considered that the market is not static, and development and expansion are to be expected. This will place greater pressure on consents and make it harder for consumers to understand them. Four submissions explicitly mentioned the need to plan for the future as consent management becomes more complex. Others referred to the development of VRPs which brings far greater complexity to payment consents.

**Area of Discussion 2: Solutions proposed**

**Education and Awareness Building:** of the 12 responses that proposed additional tools or guidance, by far the most commonly cited area was education and awareness building. This was supported by nine responses, including platforms, trade associations, and expert advisers. One piece of evidence showed that higher levels of awareness were associated with higher levels of agreement to share

data: "*Survey showed that 82% of senior SME decision makers with an existing awareness of open banking would consider sharing their data. This is compared with 56% of SMEs who had no awareness of open banking. Therefore, any tools or guidance that increase understanding and awareness of open banking is likely to be beneficial.*"

However, a word of caution is necessary. Some of the nine supporters were quite qualified in their support, with one suggesting that: "*The Future Entity could undertake some limited promotional activity, subject to specific budget/guidelines."* It would not be correct to suggest that all nine were proponents of large scale direct-to-consumer marketing campaigns.

It is also important to reflect that the discussion session held on 7 October 2022, where a number of participants highlighted the challenge of building awareness of a concept which consumers and small businesses do not understand. The minutes of that discussion suggest that: "*One consideration raised was whether consumers really understand what open banking is. An independent expert said that open banking is a meaningless term."*

This was echoed in a written submission, which stated: "*Raising consumer awareness of open banking would require substantial marketing investment. While end users may not understand or know about RFID, they do know and use contactless. Equally, increasing awareness of open banking would not [necessarily] lead to greater adoption; rather, awareness of and interest in new value propositions and use cases backed by a sound commercial model is more likely to lead to adoption."*

This leads to a related, proposed area of activity which was supported by four responses and focused on the creation of compelling and powerful stories and case studies about how open banking-enabled solutions are helping consumers and small businesses. One response articulated this as, "*working with industry to ensure customers understand the benefits of open banking".*

**Greater Transparency:** the second most common type of suggestion was to enhance the transparency of consents, both at point of sign-up and subsequently through consent management tools.

Three submissions suggested that a more prominent, templated summary of what the customer has consented to would aid transparency. This could be either emailed to the customer or be prominently available on the app or website. One of these submissions went further to call for a new "Smart Data Right" and a "Smart Data Consumer Agreement", including requirements for TPPs to put the interests of consumers first and to provide consent management tools, as examples.

Seven submissions suggested that dashboards need to evolve or be enhanced to help customers more easily manage their consents. There were a number of suggestions in this space, including the simplification of language and that VRP dashboards should be situated with other payments dashboards, to help consumers find and use these important summaries of long-lived payment consents.

One specific proposal in relation to dashboards came from an independent expert, drawing on experience from Australia. The Australian data sharing ecosystem is broader and after a review, the decision has been taken to require consent data to be shared via API. In effect, this would open the door to the provision of centralised consent management tools: *"The [Australian] Government has accepted recommendations that consent, and authorisation data should be designated as CDR data so that secure consent management services could be provided and that this also be subject to the new action initiation functionality."*

Two submissions highlighted another issue with dashboards, which is that they do not currently display the end recipient of data where that recipient is not regulated for AIS (i.e., where the data is onward shared with them). This issue is discussed in more detail in the responses to Question 9 (Onward Sharing).

**Other Proposals:** In this area, there were some additional recommendations, supported by only one or two submissions:

One submission called for a reform of the 90-day reconsent framework, suggesting that even after the FCA's recent changes, the policy still acted as a barrier to the development of effective TPP services: "*For firms to be able to assess suitability, affordability, fit, and outcome, and to monitor those principles at all times during the lifecycle of the product or service, continual data access is required. The current 90-day threshold for active consent is antithetical to that outcome, especially if consumer consent is not renewed in a timely manner. Essentially data access is cut off at that point, irrespective of the authentication still being valid."* Another submission called for a combined consent journey covering data and payments.

#### *1.19.7.3. Emerging Areas of Alignment*

Whilst there were a wide range of responses to this open question on customer awareness and education, some broad areas of commonality emerged.

With some notable exceptions, there were a number of responses calling for modest awareness and education activity, although some differentiated between awareness of open banking and open banking-enabled propositions. Few proposed major marketing campaigns to promote open ban king generically, although some did call for this on payments to create a viable alternative to cards.

On consent, only a minority proposed a more structured or transparent process at point of agreeing consent.

However, there was also a good range of submissions calling for an evolution in dashboards, as effective tools to help consumers control their consents, particularly with the expected expansion and growing complexity of the ecosystem. One brought in evidence from Australia which is opening up consent data to third parties and enabling centralised consent management. This was clearly only a single submission but given that this decision has been recently taken in Australia it would seem worthy of further consideration.

### 1.19.8. Question 9: Onward Sharing

***How can we improve the visibility over onward sharing? What is needed? (While taking into account the implication of GDPR and development of smart data legislation)***

#### *1.19.8.1. Introduction*

There was a narrower range of responses to this question, given that it referred to AIS access only and the subsequent models of onward sharing. However, there were some valuable responses and proposals for activity in this space.

#### *1.19.8.2. Areas of Discussion*

**Area of Discussion 1: Evidence of issues to be solved**

Some submissions highlighted issues in the area of onward sharing of data that required focus or resolution. In the SME space, research was supplied in one response which indicated a significant level of unease amongst decision makers about having their data onward shared: "*Our survey shows that 51% of senior SME decision-makers are concerned about the onward sharing of their financial data when sharing this via digital means. In addition, 34% are concerned that they do not have a full understanding of the data being shared, and to whom. These are clearly significant concerns and present barriers to wider adoption of open banking by the SME sector."*

Another submission from an ASPSP also suggested that the current model caused them issues in relation to managing customer queries: *"…(the bank) has experienced difficulties in addressing consumer queries or complaints in scenarios where the ultimate data holder in the chain is unknown to us, and the chain between end-data holder and TPP cannot be established."*

Beyond these two submissions cited above, there was no other evidence pointing to customer attitudes or concerns in relation to onward sharing. However other submissions did highlight a range of concerns.

One submission pointed out that this topic has had a long history of consideration and quoted sections from the BEIS consultation in 2019. This submission summarised the BEIS consultation as follows: *"The Department for Business, Energy & Industrial Strategy published the report "Next Steps for Smart Data" in September 2020, regarding the development of smart data legislation. This document mentions restrictions to onward sharing as one of the proposals made during the 2019 Smart Data review. Most respondents in the review agreed that onward sharing should be restricted, some even suggested banned entirely."*

Another submission pointed out that, "*Financial regulators like the FCA have little insight into the activities associated with onward sharing which are outside the regulatory perimeter and will not be in a position to monitor or mitigate risks to end users."* As an example of this lack of insight there was no evidence on the extent of onward sharing, with the same submission[8] highlighting that, *"[the] OBIE suggested… that 1000 parties could be involved in onward sharing, although the reality is that*

[8] The response is referencing the 2022 Open Banking Impact Report: https://openbanking.foleon.com/live-publications/the-open-banking-impact-report-june-2022/outputs-availability

*they have no way of monitoring the practice effectively."* No other submission gave any indication of the extent of onward sharing, and this was highlighted as a critical data gap.

One other submission suggested that onward sharing *"could prove to be a strategic risk to the industry"*.

A number of other responses considered there to be no issue in this space at all. In the view of many, existing regulation (such as GDPR) provided sufficient clarity and protection for consumers and no change was needed. Responses suggested that "*no customer issues arising that our members are aware of from open banking data sharing to date*" and an ASPSP similarly reported that they "*have seen no customer issues arising from open banking data sharing to date*."

One submission went further to suggest that onward sharing was a benefit to consumers and that any changes or limitations would therefore be detrimental to their interests: "*A main benefit of open banking is the availability for consumers to use a third party to securely retrieve their data and share it with another business e.g., sharing account data with a mortgage provider to enable an affordability check. Restricting this onward data sharing would unnecessarily curtail the consumer benefits of open banking*."

It is clear that this is a complex topic with a range of opinions.

One submission provides some international context to this question. An independent expert outlined the situation in Australia. "*Australia has taken a different approach to the UK in relation to onward sharing. There is no general ability to share CDR data with 'third parties' (or beyond) even with customer consent."* Onward sharing is only permitted "*to a 'trusted adviser' of the customer or if it is an 'insight disclosure".*

However, the Australian Government is currently consulting on rule changes to permit onward sharing. In the discussion session held on 7 October 2022, the independent expert suggested that *"The approach to onward sharing… was potentially too tight in the early stages which restricted adoption. It has since partially opened-up to those advising end customers, and the market is now reviewing a broader opening-up of onward sharing*".

### Area of Discussion 2: Suggested changes

As indicated above, there were a number of submissions that made the case that no change was required at all. In total, seven responses specifically highlighted that no changes were required to enhance visibility. For example, one submission stated, "*Data access and processing is heavily regulated already, including any onward sharing with fourth parties. We cannot see the need for any additional restrictions or stipulations."*

However, others did see the need for changes.

The most commonly proposed change was to improve visibility of onward sharing during consent journeys and on dashboards so that consumers were clear that their data would be onward shared to another recipient (and, by extension so that ASPSPs knew data was being onward shared). This was proposed in five submissions. Some discussed the need for different technical solutions to achieve this, some suggested that the existing Software Statement model could be used.

The next most common area cited was to enhance guidance provided to AISPs and onward shared parties (sometimes referred to as fourth parties). This was proposed in five submissions, with four

suggesting that better enforcement of the existing CEGs would be sufficient (including the provision of consent management tools) and one submission going further in calling for the creation of new standards and guidance to cover these journeys.

Beyond these suggestions there was a handful of more far-reaching suggestions. Two parties called for consent to be the only legal basis for onward sharing (with most today being onward shared on the basis of contract). This would clearly require changes to regulation.

One independent expert went even further, suggesting that "*Obligating firms to provide consent management tools would slightly improve the visibility of onward sharing. But, placing all of the responsibility on consumers to monitor, understand and consent to how their open banking data is subject to onward sharing will not provide the appropriate degree of consumer protection."*

In the view of this expert, the FCA should consider, *"Restrictions on the ability of firms to undertake onward sharing of data: This could include a blanket restriction on the onward sharing of data or if this is not possible then a restriction of onward sharing outside the FCA regulatory perimeter."*

One ASPSP proposed the longer-term development of *"technological solutions to tracking data (and meta data) need to be explored by industry".*

#### *1.19.8.3. Emerging Areas of Alignment*

This was an area with three quite clear schools of thought and therefore limited areas of alignment. The three schools of thought can be summarised as follows:

- **There is no evidence that significant issues are occurring in this space. Existing regulation provides sufficient checks and balances, and onward sharing is beneficial to the development of the ecosystem. It should be allowed to continue as today.**

- **Onward sharing is not always clear to consumers and small businesses today and we should evolve guidance and control tools to make it more visible.**

- **Onward sharing is a significant risk to consumers, and we should evolve regulation to control onward sharing more tightly, limit it or stop it altogether.**

Broadly speaking we can estimate that seven responses fall into the first category, five into the second and four into the third. Others did not provide a response.

### 1.19.9. Question 10: Key player relationships

***What needs to be done to define and clarify the roles and inter-relationships of key players in the ecosystem, including firms the information is onward shared with, as well as Pay.UK and retailers?***

#### *1.19.9.1. Areas of Discussion*

**Area of Discussion 1: Lack of clarity on roles and obligations**

The primary gap identified by several participants was a lack of clarity around the roles and obligations of parties who are in receipt of data that has been onward shared. This issue is extensively discussed in the responses to Question 9 in the preceding question. Apart from this, the overwhelming majority of respondents were of the view that ecosystem roles are clear and governed by PSD2 and, in respect of information sharing and security, GDPR and other UK Data Protection legislation together with ongoing regulatory oversight. It was noted by one platform that new roles are likely to emerge as the ecosystem evolves, not all of which can be envisaged at the outset.

An independent expert underlined the need for oversight of all parties within the ecosystem. The Standards setting authority requires authority over all parties within the ecosystem, to enforce monitoring and compliance. It was noted as a comparable example that the Pensions Dashboard ecosystem has more control over all parties in the ecosystem. It was suggested that the open banking ecosystem does not yet have the right roles and responsibilities defined and in place to mitigate the potential risk resulting from a complex multi-party, ecosystem. It was noted that this could lead to consumer detriment.

One respondent suggested that the role of retailers was not well defined and because they fell outside the regulatory scope of the FCA, there is no compulsion for them to conform with any standards or requirements that protect customers and ensure high quality journeys. It was suggested that there would be benefit in clarifying expectations and making that visible to end-users.

Anther respondent thought that it would be useful for regulatory clarity on what is in the regulatory domain and what is in the commercial environment for the market to agree. Another respondent felt that the relationship between Pay.UK and the OBIE for the CoP service could be further clarified to ensure effective engagement with all firms.

#### *1.19.9.2. Emerging Areas of Alignment*

Broadly, with the exception of the issues on onward sharing, there was broad agreement that roles are well defined. The question raised by expert advisers as to how to ensure that participants are encouraged or compelled to diligently fulfil those roles remains a matter where there are divergent views.

## 1.19.10. Question 11: Delivery of key ecosystem capabilities

***What capabilities/functionalities are needed for the ongoing successful operation of open banking? What may need to be provided centrally by the Future Entity (or another entity) versus distributed? Please provide rationale and evidence.***

### *1.19.10.1. Areas of Discussion*

**Area of Discussion 1: Central or outsourced provision**

There were a significant number of core capabilities mentioned in responses that can be categorised as follows:

**Standards Development:** there was unanimous agreement that maintaining and evolving existing Standards and introducing new versions of the Standard as required by the ecosystem or regulation was a core capability which there is a continuing need for. A widely held view was that fragmented rules and standards present a risk and could impact user journeys.

All respondents envisaged that this core activity should continue to be provided centrally. One trade association argued that the centralised model underpinning these sorts of services to-date had required significant investment over a prolonged period and this should be leveraged in any future developments.

One ASPSP considered that it would be efficient to have a specific entity serving both open banking and open finance providing a "*centre of excellence for standards development, over time spanning many industry sectors*". Given the broad reach but specific mandate, it was recommended that this body should be small and not carry out operational activities which would make governance and funding structures unwieldy for an expansive cross-cutting mandate. It was suggested that this could be either government funded (as in Australia), or an independent membership body (ETSI in the EU, or the Open ID Foundation in the US). A trade association agreed that a composite cross-sector Standards body would result in a Standards design that was interoperable across the entire economy, which was likely to result in cost reduction and maximisation of end consumer benefits.

Several respondents stated that Standards development would need to cover both regulatory and commercial drivers. This would require supporting governance arrangements that can effectively prioritise demand and resolve competing priorities.

One platform suggested that there would be merit in Pay.UK having responsibility for open banking rules and Standards giving it the ability to holistically manage Faster Payments systemic risks. Several TPPs expressed concerns that the relationship that Pay.UK has with banks would result in a conflict of interest and that Pay.UK has several other competing priorities. In the discussion session on 7 September 2022, it was clarified that Pay.UK is independent and could therefore support open banking payment API standards in the future, although this would require an increase of resource.

**Conformance Services**: the majority of TPPs feel that it is critical to have an independent monitoring function to ensure conformance with regulatory Standards is achieved. However, there were divergent views expressed by ASPSPs. One ASPSP and a trade association questioned whether this service is necessary given that other more developed payment methods are regulated by the FCA and the PSR without a separate conformance body.

Most other ASPSPs accepted the need for monitoring to ensure high-quality and consistent journeys for customers, but considered that conformance monitoring testing, and collation of MI should be

applied consistently across the whole ecosystem. They envisaged that a central provider would play a co-ordination role collating data/information from participants, with monitoring and any enforcement action being taken by relevant regulators.

One ASPSP recommended that an ecosystem performance strand of activity should include collection and review of market data to understand trends, emerging areas of customer detriment to inform future Standards development, operating model requirements, or needs for regulatory support. They recommended that this would be best achieved via a financial services focused entity with cross-industry governance and funding, providing "scheme" services across open banking /open finance.

**Trust Services:** there were widely diverging views as to whether this should be a centrally provided service. ASPSPs, one platform and a trade association suggested that alternative models for participant identity verification could be more efficient, operate at lower cost and reduce concentration risks. They argue that the current approach lacks scalability and is not sustainable, and a federated trust/identity framework like the eIDAS model used for PSD2 in Europe could be easily scalable for open finance. They stated that there are many Certificate Authorities in the market (some of which they are using for the provision of their EU activities), and the underlying technology is available at a lower cost. Commercial supply of these services resolves financial liability risks.

Most TPPs support centralised provision of trust services as they are considered critical infrastructure since Brexit because of the use of a UK alternative to eIDAS certificates.

**Participant Support**: there was support from many TPPs and some ASPSPs for testing and certification support services which reduce the cost and complexity of integrations between parties. TPPs saw a continuing need for provision of a service desk which enables action to be taken on issues with API performance impacting open banking. One ASPSP saw the need for centralised coordinating activity as new services are deployed across a complex ecosystem. However, as these services embed the focus shifts to direct interaction between counterparties to enable resolution of residual issues and the need for centralised operational support at inception could fall away.

One trade association argued that these services which are currently centrally provided will continue to be relied upon by participants and should be protected, as change may introduce barriers to ASPSPs and TPPs looking to operate within the boundaries of the CMA Order or PSD2.

**Multilateral Agreement Support**: several respondents (TPPs, ASPSPs and trade associations) saw the specific need for the orchestration of MLAs to enable the success of A2A payments in retail. This would include dispute management rules and processes for A2A payments. They identified the need for scheme-like supporting activities to facilitate the successful growth of open banking and open finance, which were mainly self-regulated and industry-led. One ASPSP suggested that this warrants the establishment of a financial services focused entity with cross-industry governance, funding and membership, to support open finance with activities and rules in each vertical (such as open banking data or open banking payments).

One ASPSP suggested that this entity might be treated as a payments system operator or that Pay.UK might fulfil this role.

**End User Needs:** expert advisers stated that the Future Entity will need to have strong end user representation, should undertake research, and consult end users and perform the role of educating users about the use of open banking and what they need to do to protect themselves.

#### *1.19.10.2. Emerging Areas of Alignment*

The key area of alignment was around the continuing need for Standards provision and Participant Support, although there were a range of views on how to achieve this. There is broad agreement that the lessons from other international jurisdictions suggest that a strong, clearly defined organisation in place to drive change, and consider the views of users, results in better progress. It was agreed that in the next series of sprints as we move into the "how" phase, consideration of the future funding model will be critical.

# EVIDENCE AND FINDINGS FROM THE SECOND ROUND OF STRATEGY SPRINTS

## 1.20. Second Payments Strategy Sprint

### 1.20.1. Section 1: What do we need more evidence on?

***QUESTION 1.1***

***There is a need for evidence and data in relation to open banking payment success under different value and use cases, as well as data identifying reasons behind payments not going through.***

a) **What metrics and data in relation to payment success should be collected?**
b) **Who should provide this data – Banks / TPPs / Both?**
c) **How should this be operationalised, including who should take this forward, in the short-term and on an ongoing basis as open banking+ develops?**
d) **Should this insight be shared across ecosystem and what is the best way to do this?**

***QUESTION 1.2***

***Possible / perceived level of fraud risk was highlighted as key barrier to adoption for priority use-cases, including high-value payments, non-sweeping VRPs and retail transactions. We have asked the data sprint to outline the data points that TPPs and ASPSPs would need to provide to enable us to form a better view of the state of play today and case studies for where fraud has taken place. We would welcome the payments sprint attendees to provide key data points, case studies and vulnerabilities.***

***QUESTION 1.3***

a) **What is needed to make open banking payments a viable business case for banks?**
b) **To what extent does the fixed fee for Faster Payments make open banking payments more expensive for retailers than card payments, and how much of a problem is this?**
c) **If any, which aspects of the commercial model require regulatory intervention?**

#### *1.20.1.1. Areas of Discussion*

**Area of Discussion 1: Suggested Payment Completion Metrics**

Respondents suggested that the following metrics would provide valuable relevant insights into payments:

1. **The volume and value of payments initiated by a PISP per ASPSP API channel that succeed or failed and why (banded by transaction value). It was noted that success rates vary significantly depending on whether they are web- or mobile-based.**
2. **Average transaction value of failed transactions per defined use case.**
3. **The volume and value of PISP initiated payments the sending FPS institution (ASPSP) made available to the PISP in near real time.**
4. **Real-time information as to whether the funds are accepted by the beneficiary customer.**
5. **Breakdown of failed payments by failure reasons. Several TPPs and some banks noted that error codes are often generic or not applied at all, which inhibits the ability to determine accurate picture of what is causing errors following failed redirections for**

**transactions from ASPSPs. These respondents recommended that error codes should be standardised across industry. This issue is discussed in more detail in at Section 4.2.3.**

6. **In addition to assessing payment success rates, one bank indicated that it would be useful to collate comparative payment completion data for A2A payments initiated via direct channels vs. A2A payments initiated via PISPs, fraud losses (per £ of value transferred) for direct and PISP-initiated A2A payments, and intervention rates and false positive rates for direct and PISP-initiated A2A payments.**
7. **One TPP suggested that it would be useful to have a centralised database of payment limits applied by ASPSPs, as while some payment limits are currently published, this is not comprehensive or detailed. Improved transparency would enable a significant number of failed payment attempts to be avoided.**
8. **Some TPPs indicated that it would be beneficial to see reporting of all individual transactions which were classed as fraud, this would enable PISPs to work collaboratively with banks to identify the cause of the disputed transactions. It was suggested that a working group is established to assess each of these payments.**
9. **It was noted by several respondents that there will naturally be some dropouts when consumers change their minds, accidentally close windows or intentionally abandon a payment, which are hard to determine from available data. Broader consumer research will be required if broader issues of abandonment are to be explored.**

One bank stated that there was no evidence that additional data is required to measure the efficacy of open banking payments and that any requirement for incremental data should be evidence-based and at a sufficiently granular-level to determine where there are genuine shortfalls in the current payments journey within the control of TPPs or ASPSPs

A number of TPPs noted that the OBIE had recently undertaken a data gathering exercise to explore the relationship between failed payments and technical errors. The findings of this should be considered by the Committee once the analysis is completed.

### Area of Discussion 2: Who should provide this data?

It was noted that dropouts in payment journeys occur at various stages, with many of the potential break points occurring prior to any involvement of the ASPSP. Opinion was divided as to the value of providing data regarding those elements under the control of TPPs. Several TPPs noted that there were considerable differences in the approach to this – some TPPs offer a simple 'bank button' on checkout and almost immediately redirect to the bank, while other providers have several screens between selecting the payment method and being redirected. Increasingly, TPPs are also beginning to differentiate between new users' and returning users' payment journeys. It was argued that these two factors would make comparing pre-redirect performance meaningless between TPPs.

However, most respondents considered that there would be merit in looking at root causes of failure holistically. This would require granular level data from both TPPs and ASPSPs and a degree of standardisation to enable appropriate comparisons to be taken as different performance metrics would be expected for different use cases. Without a complete set of data covering end-to-end performance, it would not be possible to empirically evidence issues and determine remediating activities.

### Area of Discussion 3: How should this be operationalised?

The majority of respondents indicated that there should be a coordinated, ecosystem-wide approach to data sharing, with the OBIE or a Future Entity (or entities) playing a central role in operationalising data collection from relevant parties and the use of data and metrics. One bank noted that this should be a Future Entity activity as it is non-Order related. This respondent also noted that alternatively UK Finance could collate the MI from ecosystem participants.

Consumer experts concluded that to make rapid progress in this area, it was likely that regulators would need to impose clear reporting requirements on both banks and TPPs, with prescribed data requirements and reporting periods, with data submitted to an independent body for monitoring, analysis and publication. In their view, these functions could naturally be carried out by the Future Entity, but it was noted that in order to discharge this role effectively, it would need regulatory backing to request additional data, and to undertake more focused monitoring activities to interrogate issues in detail where required.

One ASPSP suggested that in order to avoid duplication and fragmentation, regulators should augment existing reporting mechanisms such as the existing fraud reporting under REP017 and PSR specific directions to cater for this additional data needs. This would ensure a whole of market view is available, rather than a data set limited to just CMA9 firms.

### Area of Discussion 4: How should data be published?

It was noted that API performance metrics are already shared publicly, and this could be extended to the wider ecosystem. Most respondents felt that data should be published in aggregated and anonymised form. However, one consumer expert noted that the PSR is proposing mandatory firm-by-firm reporting on APP fraud and considered that this would be a good model to follow, particularly as it provides a competitive impetus for firms to improve performance.

One bank recommended the creation of a real-time dashboard that provides whole-market visibility and more detailed failure reasons for incomplete transactions.

### Area of Discussion 5: Fraud data & risks

There was broad agreement that fraud risk needs to be considered at a much more granular level, recognising that there are considerable variations between fraud vulnerabilities at a use case level.

Open banking is vulnerable to all types of fraud but also at particular risk from APP fraud as seen in other digital channels.

Further evidence was received from several banks demonstrating that loss/turnover ratios for open banking transactions are 5x higher than other faster payments digital channels, and 3x higher than other digital channels. It was suggested that this will become more challenging as open banking payment activity increases and use cases diversify. However, one bank challenged the premise that there is a higher fraud risk associated with open banking payments.

One bank felt that inherent weaknesses in the approach to open banking payments that could introduce fraud risks are:

- **the expressed intent to reduce friction in PIS journeys, which can inadvertently induce fraud to migrate to those channels**
- **the lack of requirements or enforcement of open banking specifications and rules beyond the CMA9**

- **the level of information provided to PSUs by TPPs, and the quality of their KYC controls to minimise the risk of APP fraud.**

This respondent noted that while TPPs have focused on reducing friction in the payments journey, they, as well as ASPSPs, remain responsible under the Consumer Duty to ensure the inclusion of "…appropriate friction in customer journeys to mitigate the risk of harm and give customers sufficient opportunity to understand and assess their options, including any risks." (Consumer Duty, Section 9.3). It was also noted that high TPP default payment limits (for example, £1000 for an end-of-month savings round-up) in relation to VRP consents could present a control weakness and give rise to APP fraud.

Most TPPs indicated surprise at the relevant evidence put forward by other respondents in the Interim Report suggesting that there was a higher level of fraud in open banking payments relative to other channels. They argued that expert advisers should review relevant evidence and there are existing data reporting mechanisms which could enhance the provision of fraud data:

1. **The FCA REP017 reporting requirements, which can enable the publication of aggregated fraud data.**
2. **UK Finance half-yearly fraud report, which could be expanded to include fraud data in open banking.**

It was noted that the OBIE, via an established Security and Fraud Working Group, had gathered intelligence on fraud and vulnerabilities. It was recommended by some respondents that this group is reconvened to look at fraud-related data in open banking.

One TPP recommended that both ASPSP and TPP should cease sending payment links by SMS/email and noted that this practice has been prohibited by regulators in markets such as Singapore.

### Area of Discussion 6: Commercial incentives for banks

One platform provider argued that the market should be allowed to determine commercial frameworks and that there is no need for regulatory intervention. Banks generally agreed with this point of view, arguing that there needed to be sufficient incentives to invest in new products or services. However, most TPPs believed that there were insufficient commercial incentives for banks to invest in enabling TPPs to initiate more open banking payments, given the revenue that they make from card-based interchange fees, and that some form of regulatory intervention was therefore required.

Specific points of note were:

**Business case:**

- **Most TPPs challenged the assumption that it was necessary for banks to have a commercially viable business case. They noted that legislative and regulatory action was originally viewed as necessary precisely because it was unlikely to be achieved voluntarily by banks. Their view was that the purpose of open banking is to increase competition in banking and payments to the benefit of businesses, consumers and the wider economy. They argued that the continued focus should be on what is required to maximise the value of open banking for end users.**

- **A few TPPs stated that, as banks are already remunerated for accepting open banking payments through their charging for incoming Faster Payments, the appropriate market-based mechanism would be through varying this charge rather than charging the open banking payment provider for access to an API.**
- **Banks stated that they are incurring costs to maintain the infrastructure and processes necessary to support open banking payments. They argued that allowing charging for payment initiation would provide incentives for further investment and promotion of A2ART and premium discretionary APIs. It was noted that irrecoverable investments made, and costs incurred, in supporting open banking, have implications for other services provided by banks.**

**Banks argued that payment services beyond the CMA Order need to be financially sustainable, providing both ASPSPs and TPPs with the means to recuperate investment costs, ongoing operational costs and sufficiently compensate for a loss of income from existing services either directly (equivalent pricing) or indirectly (reduced operational or processing costs). It was widely noted that the current risk/reward asymmetry (under which the banks bear most of the risks and costs associated with A2A payments without rewards, whilst PISPs are able to reap most of the rewards with few costs/risks), has resulted in ASPSPs having little incentive to invest in open banking payments today and in innovation tomorrow. One bank noted that this asymmetry would be exacerbated by PSR's proposed approach for the reimbursement of APP fraud, and hence strongly support the exclusion of open banking payments in this initiative, at least initially, to give the industry time to consider sustainable purchase protection models.**

**Purpose of regulation**

- **Many TPPs further argued that allowing banks to charge for access to payment accounts in order to initiate payments (whether SIP or VRPs) is contrary to the purpose of the PSRs and the CMA Order, and would lead to a less competitive market. In their view, at the present time as there is not a positive business case for banks, since they would lose more from lost interchange revenue from card payments than they would gain from more Faster Payments revenue, therefore, regulatory intervention was needed.**
- **Some TPPs noted as an example that currently only one bank has indicated they are interested in supporting non-sweeping VRPs.**
- **An independent expert recommended regulatory intervention to prohibit payment card interchange fees, as a possible solution to this issue.**

**Need for consistency and standardisation**

- **Some TPPs expressed concern that reliance on bilateral agreements between PISPs and ASPSPs in relation to dispute management, liability, and consumer protection might result in differential and fragmented services for consumer, reducing the attractiveness of propositions to end users and merchants. Some suggested that a thin rulebook between ASPSPs, PISPs could usefully create a common foundation that would build consumer and merchant trust in VRPs, encouraging adoption and innovation.**
- **Some banks agreed with TPPs that regulators would need to support the creation of MLAs covering liability and charging issues. They considered that it was important for these issues to be settled as a matter of policy, so they were not subject to challenge or**

**uncertainty, which could adversely impact adoption, investment, and innovation by participants.**

- **Banks generally felt that the consideration of minimum consumer protections for A2ART transactions may also require both regulatory and public policy consideration.**

#### Area of Discussion 7: Impact of Faster Payments fees

The Faster Payments Scheme charges bank participants on a cost-recovery basis and are currently around 1.5p per payment (for a send or a receive). It was noted that this is unlikely to change significantly once the New Payments Architecture's new clearing and settlement service is procured and implemented.

An independent expert made the point that these fees are not directly comparable to payment card interchange fees as they represent a cost rather than an income to banks.

No respondents saw a pressing need for intervention in this area.

### 1.20.2. Section 2: What can we do in the short-term?

#### *1.20.2.1. QUESTION 2.1: Enabling high value payments*

***What are the short-term solutions to enable high-value payments to be made consistently through open banking? What are the costs and benefits associated with those and what are the challenges to implementation for ecosystem participants? The FCA clarified that firms should not discriminate against open banking and ASPSPs are expected to allow each customer to initiate a payment via a PISP to at least the same level of functionality that is available to a customer if they initiate a payment through direct channel(s).***

#### Introduction

Secretariat received evidence on a number of inter-related areas relating to increasing the proportion of successfully completed high-value open banking transactions, an issue highlighted by a number of TPP participants during Sprint 1.

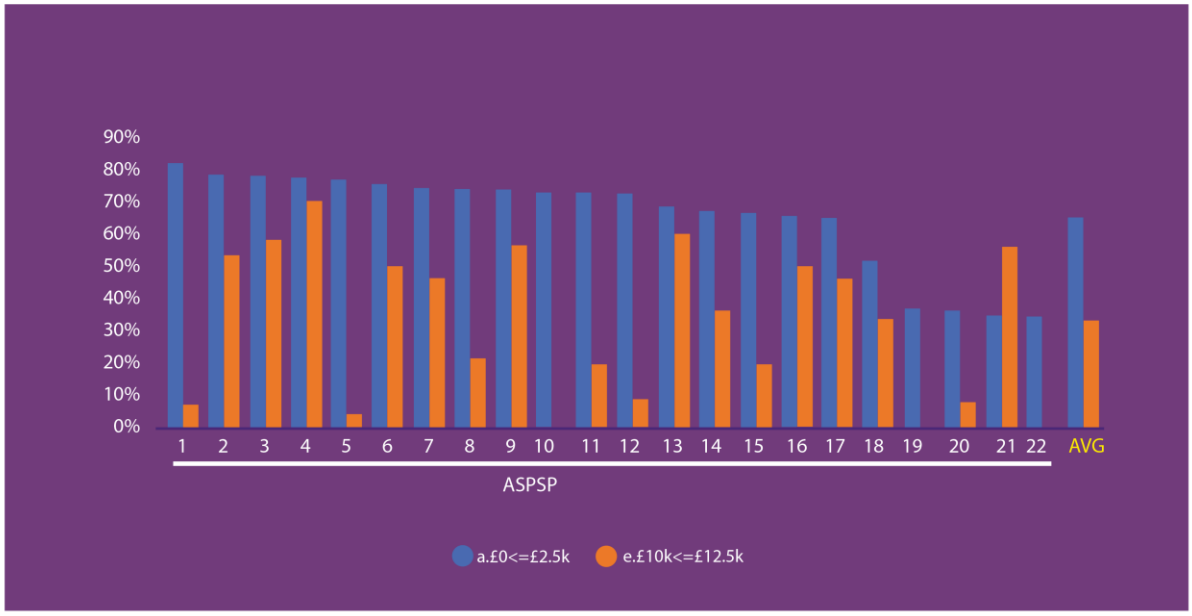
However, two ASPSPs challenged the premise of the questions in the first place. One ASPSP stated: "*High-value PISP transactions account for a very small percentage of PISP transactions. Without any evidence being presented to date, we're unable to comment on why this is seen as a high-priority item in the unlocking of account-to-account transactions. Considering the cost-of-living crisis, we would suggest high-value payments will become irrelevant for an increasing proportion of PSUs*."

Another ASPSP quoted experiences from their PISP business which had not identified particular issues with high-value transactions: "*[Our] PISP proposition successfully supports multiple merchants with higher value transactions (£10k ATV), and we have not found specific obstacles preventing the adoption of high-value use cases."*

These two pieces of evidence are in contrast to data provided by members of the TPP community which demonstrate fundamental challenges with high-value payments. For example, one TPP submitted evidence of conversion rates by ASPSP and by value. This found that across 22 ASPSPs the conversion rates dropped from 65.4% for transactions under £2,500 versus 33.8% for transactions

between £10,000 and £12,500. We summarise the data points by (anonymised) ASPSP in figure 7 below:

***Figure 7. Conversion Rates by ASPSP: Under £2,500 vs £10,000 - £12,500***




*Source: TPP submission, reproduced with permission.*

### Areas of Discussion: Proposed Solutions

Unsurprisingly, given that this is a critical issue across the ecosystem, we received a wide range of proposed solutions, focused into two main areas: the implementation of TRIs, and addressing perceived issues with payment limits.

- **TRIs:** 10 submissions cited implementation of TRIs as a potential solution to resolving the issues with high value payments. This included responses from seven TPPs and three ASPSPs. There were fewer clear views on how to effectively introduce TRIs, with four responses suggesting that their use should be mandated to ensure whole of market coverage: *"[TRI] value will only be realised if their use is widely adopted, or even mandated, as they arguably have minimal value unless they are used on a consistent enough basis to be relied upon [as] part of the payments process."* Other responses did not go as far as suggesting TRIs should be mandated, but instead proposed that there should be a managed roll-out process.
- **Payment Limits:** eight responses highlighted resolving low (for some TPPs' propositions) payment limits as important. Work to address payment limits was more common in TPP submissions, featuring in seven TPP submissions and only one ASPSP's. A typical quote in support stated: "*ASPSPs must be closely monitored by regulators/the Future Entity to ensure that their anti-fraud processes minimise false-positive payment interruptions… and meet equivalence regulations.*"

  There were a wide range of proposals for dealing with this, ranging from expanded

monitoring, mandated and consistent payment limits (for example, all banks to have a payment limit of £25,000 for open banking payments) or a simpler option of transparency of payment limits. Some respondents from banks were, however, passionate about the need for banks to be able to set their own payment limits in line with their own risk appetite and the risk profile of their customer base: *"At present we cannot support any regulatory intervention that would prevent our ability to implement fraud controls due to the significant liability associated with APP scams in the UK, particularly for high-value payments."*

Beyond these two core common suggestions to address the issues identified, there was a longer list of potential ideas for consideration by the Committee, including:

- **Risk-sharing**: three responses suggested that the ideal solution would be one in which risk was shared between ASPSP and PISP, for example: "*A methodology to allocate liability to a PISP within a payment chain would act as an incentive on PISPs to build in fraud prevention measures commensurate to the risk of HVPs."* This was acknowledged to be a longer-term solution however, probably requiring some form of contractual arrangement. One bank and a platform stated that the only long-term solution to this challenge was an MLA.
- **Whitelists**: two responses suggested the use of whitelists, so that ASPSPs could allow higher value transactions to proceed in payments to known trusted recipients, such as HMRC, government departments or large retailers which had undergone additional verification.
- **Error codes and data**: a few TPPs stated that better error codes would help PISPs manage issues better with their customers; and better data across the market would help policy makers and regulators to properly analyse the issue.

### Potential Areas of Alignment

There is broad agreement that this is an important area to resolve, although its complexity was clearly acknowledged in responses. Whilst we had 10 responses which supported TRIs and eight supporting some form of action on payment limits, there were a range of views on the way forward on payment limits.

### *1.20.2.2. QUESTION 2.2: Providing payment certainty*

***Sprint 1 identified three ways in which the ecosystem could provide additional payment certainty to PISPs and merchants. What are the pros and cons of each of these three options? What are the implications on development timelines?***

a) **Enhanced payment status messaging.**
b) **A new functionality in which a payment is either initiated immediately or not at all.**
c) **A new functionality in which a PISP is able to obtain a payment guarantee, with settlement occurring later.**

#### Areas of Discussion

Overall, enhanced status messaging was most broadly supported across the ecosystem of these three potential solutions. In total, 11 submissions favoured this of the three proposed solutions, including four ASPSPs, one payment platform and six TPPs. One TPP described this as "*a crucial part of improving the payment certainty for merchants*". Potentially, support could have been higher as a number of TPPs understood the question to refer to status messaging within the Faster Payments Scheme, whilst the intent of the question concerned the provision of such messaging from ASPSPs to TPPs. One quote, from a bank, summarises the position well: *"We would welcome the FCA encouraging or mandating adoption of final payment status messages across all UK ASPSPs as a short-term solution to the problem statement above."*

In contrast, the other two potential solutions received much more limited support, partly because they were considered by many to have long-term lead-times. Three supported "now or never" payments (option b) and two supported some form of payment guarantee (option c). One bank submission estimated that both option b and c would take *"c.24 months from initiation to delivery, depending on the complexity of requirements"* and this would give it a *"limited life before the NPA is delivered".*

A common theme in commentary was that both option b and c should be provided within the NPA and not be considered as specific open banking payments functionality. A typical quote stated: *"Instant Payments are being developed as part of the NPA. Trying to deliver an equivalent service for open banking would not be the right thing to do. Open banking needs to ensure alignment to the industry developments, not run in parallel."*

#### Potential Areas of Alignment

There was broad support for work to improve the consistency and accuracy of status messages provided from ASPSPs to PISPs, and this was considered by many to be deliverable within the short-term time period defined by the Committee.

Other functional enhancements, whilst they offered clear utility for some, were considered by most to be long-term initiatives. Many highlighted that, as such, they should be considered part of the NPA and not as open banking initiatives given the time it would to take to develop such capabilities.

### *1.20.2.3. QUESTION 2.3: Error messages*

***We have asked the ecosystem sprint to consider error messages and in particular the additional fields needed, and the costs associated with those. From a payments perspective specifically, please highlight if there are any messages of particular importance.***

#### Areas of Discussion

The first question addressed in the evidence is whether the current implementation of error codes is acting as a barrier to effective TPP payment solutions or in their ability to support their customers. Only one response suggested that there were no issues with the current implementation, from an ASPSP with a PISP service: *"As a PISP we have found the Open Banking Standard fit for purpose in terms of the error messages it supports."* This was strongly countered by other voices who explained in evidence how inconsistent implementations of error codes or lack of detail acted as a key barrier. For example, one TPP stated that: "*For authorisation failures, we have found that 91% of errors and their error codes do not provide enough information for … [us] to communicate to the customer what went wrong."* This was reinforced in other submissions, for example: "*Currently, many of the bank APIs provide generic error and fail messages which makes it impossible for PISPs to correctly handle customers."* An independent expert underlined the importance for consumers to get clear and consistent messages from banks and TPPs.

As this analysis makes clear, the issues here are a complex mix of areas of potential enhancement in the standard and lack of consistent implementation across all ASPSPs in the market.

Ten submissions called for enhanced payment failure messages to be provided and a number also called for greater consistency across all ASPSPs. One submission suggested that such improvements would be a low priority. The rest indicated that this was an area of importance for their business and their interactions with their customers.

One ASPSP identified a new error message which it required as part of the VRP standard, when "*a payment fails due to being outside of the parameters of the VRP mandate".*

Another submission highlighted the technical and complex nature of this issue and suggested that: "*A technical working group – made up of industry subject matter experts – be convened to develop proposals for future usage.*"

However, two ASPSPs, whilst accepting that there may be value in this work, issues such as anti-money laundering, fraud and GDPR needed to be considered: *"Any development of enhanced messaging should consider the implications on GDPR, data privacy, fraud and AML controls and the requirements in the Payment Services Regulations 2017 on notifying a refusal to make a payment."* One included a note of caution: "*As an ASPSP we would challenge the appropriateness of introducing error messages disclosing information about the reason for a payment rejection; these could be exploited by fraudsters to reverse engineer banks' transaction monitoring models."*

#### Potential Areas of Alignment

While recognising one dissenting voice, there was a general agreement that the current implementation of error codes leaves significant gaps from a TPP perspective, with knock-on impacts on end users. Several candidate solutions were proposed, with some alignment work taken forward in a technical working group, where issues such as AML, GDPR and fraud could also be considered.

### *1.20.2.4. QUESTION 2.4: Non-sweeping VRPs*

***Are there any non-sweeping VRPs use-cases which ASPSPs could accept without further standards being in place and MLAs (e.g., covering protection)?***

***What are the costs and benefits associated with the different options to enable VRPs to develop further proposed by members, namely regulated fee cap or pricing model, requirement for all to develop non-sweeping VRPs, treatment under Faster Payment as single payments, etc?***

#### Areas of Discussion

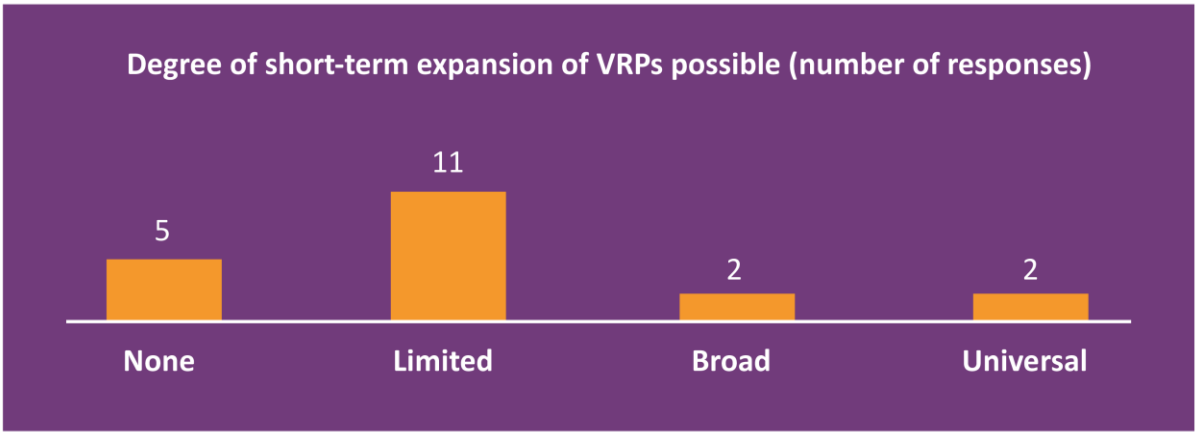
There are two broad areas of evidence to consider here:

- **Is an expansion of VRPs beyond sweeping possible in the short term?**
- **What are the costs and benefits of the various options to further develop VRPs?**

#### Area of Discussion 1: Is an expansion of VRPs beyond sweeping possible in the short term?

There was a wide spectrum of views in evidence, ranging from those that saw no potential for expansion in the short term, through to those who considered it was possible to move to a full expansion beyond sweeping. However, overall, the responses can be represented as follows:

***Figure 8. Degree of short-term expansion of VRPs possible (number of responses)***




As illustrated above, five responses considered that no expansion of VRPs was possible versus 15 that considered it was. The five which said that no expansion was possible included two ASPSPs, two expert advisers and one TPP. The consumer expert adviser position was based on the lack of consumer protection, which in their view precluded any expansion beyond sweeping.

Amongst those who supported some form of expansion, limited expansion was clearly the most popular position, with responses highlighting specific lower risk sectors such as utilities (three), government payments (three), international sweeping (two), investments (two) and charities (two). While overall, it is clear that submissions favouring short-term expansion were skewed towards TPP

responses, two large ASPSPs considered that this was feasible. The four responses envisaging a more significant expansion were all TPPs.

### Area of Discussion 2: Costs and benefits of options to develop VRPs

This question considered both fee arrangements and regulatory structures required to enable the development of VRPs. A number of responses did not submit evidence relating to fee arrangements because of competition concerns and this summary is therefore not fully reflective of the views across the ecosystem.

On the question of regulatory mandate, a number of submissions saw this as essential. One TPP stated that "*[the expansion of VRPs] will not happen without further regulatory intervention*". Another stated that: "*Mandating all to develop non-sweeping VRPs should happen, and is important for the success of open banking uptake".* Overall, seven responses set out the need for non-sweeping VRPs to be mandated: six TPPs and one bank.

However, there were other strong voices calling for the expansion of this functionality to be left to the market, including this example from a platform: "*In terms of non-sweeping VRPs, the market should be allowed to develop the commercial environment. There is no need for regulatory intervention at this stage in the lifecycle of open banking payments."* Overall, four responses clearly set out their opposition to regulatory intervention. Other responses were either unclear on this point or did not state a view.

Some submissions (two) also called for the development of an MLA to support development, with one of these describing it as a "thin rule book". This area has been extensively covered in other questions, so it is perhaps not surprising that few provided evidence on this point.

Some submissions provided views on pricing, although others remained silent, in some cases due to competition concerns. Six responses, all from the TPP community, called for a fee cap on the price that ASPSPs could charge PISPs, set by the regulator. There was one TPP submission which recognised issues both with price-capping and commercial solutions based on pricing-for-access, suggesting that access should be free with banks being able to gain revenue through competitive pricing for inbound Faster Payments, in a similar model to Direct Debit pricing.

### Potential Areas of Alignment

Evidence submitted to this question highlighted a number of areas of fundamental difference between groups:

- **For expert advisers, the overriding concern is consumer protection, and no progress can or should be made in this area without considering and resolving this issue.**
- **For many, but not all TPPs, some form of mandated expansion of VRPs is required. No ASPSPs supported this.**
- **A number of TPP submissions favoured price caps for VRPs. ASPSPs commented more broadly about market-based solutions.**

However, despite these differences, it is striking that most responses considered that it was feasible to expand VRPs into a number of low-risk sectors such as government payments, investments and charities, provided that appropriate solutions can be found to the differences outlined above.

### *1.20.2.5. QUESTION 2.5: First port of call (disputes)*

***For purchase risk disputes should the ASPSP be the first point of call (as is the case under the payment services regulations)?***

#### Areas of Discussion

The majority of responses favoured the first point of call being the merchant, not the ASPSP. This was proposed in 12 responses, with seven suggesting that the existing structure was appropriate. There was no particular pattern in responses, with four TPPs saying that ASPSPs should remain the first port of call and five saying that the merchant should be first port of call.

Reviewing the responses in detail, it seems quite likely that two factors limit the clarity of responses. Firstly, this question is inextricably linked to issues of consumer protection and dispute resolution. Some responses gave significant detail on how dispute management should evolve, and clearly a new structure for managing payment disputes would influence the first port of call for consumers.

Secondly, there are potentially some definitional issues in what constitutes a "purchase risk dispute". One response defined it as being a scenario where a consumer "*has unsuccessfully disputed a purchase with the payment recipient (payee, e.g., merchant), namely, the merchant has refused to offer a refund or other resolution to the dispute, then, yes – the consumer's ASPSP should be the first point of call".*

This final quote exposes a level of ambiguity in the definition which may influence responses. If a consumer has not received an item that they have paid for, it would be common practice to contact that merchant. The subsequent question is what a consumer should do if the merchant refuses to resolve the issue, but the evidence provided no clear views on this.

#### Potential Areas of Alignment

Whilst responses appear to show a 12 / 7 split and therefore minimal consensus, it is likely that there is greater alignment than this simple analysis suggests. Moving forward on this topic will be inextricably linked to questions of dispute management and consumer protection and given responses to other questions and input from the Sprint Discussions, the evidence suggests that many respondents would support this broader area being a priority for resolution.

We note that the Ecosystem Discussion Session held on 25 November 2022 presented a summary of evidence suggesting that there was, *"broad consensus on a need for some form of activity to enhance disputes for payments, but no common view on whether this should simply be a rule book and managed in a decentralised way, or a centralised function"*. There was no challenge to this summary in the session.

### *1.20.2.6. QUESTION 2.6: Batch and multiple payments*

***Some respondents talk through the need to develop solutions for batch and multiple payments, in particular for SMEs.***

**a) Is this a priority and what are the associated pros and cons of enhancing the Standards?**

**b) If so, how can this be done practically?**

**c) Are additional standards needed and how quickly could it be developed?**

### Areas of Discussion

We received a small number of very detailed submissions on this, signifying the specific nature of this issue. The responses received indicate a clear lack of alignment, with eight indicating it was a priority for enhancement and nine indicating it was not. Within this it was notable that all six large bank responses indicated that this was not a priority area in their view. One ASPSP submission acknowledged that whilst "*APIs already exist… the customer journey is poor. Under PSD2 there is no incentive for ASPSPs to make the journey better because of inability to recover the investment required."* This requirement for ASPSPs to make a commercial return to justify enhancement was a common feature. Another ASPSP submission suggested that enhancements should await the roll-out of the NPA.

On the other hand, the nine positive responses made a clear case that enhancing the standard "*would have a major positive impact on SMEs*", particularly in use-cases such as payroll, bill paying and regular recurrent payments.

One submission provided interesting detail on the way in which such payments are evolving outside the Open Banking Standard. This submission noted that "*several banks have independently invested in building bulk APIs i.e., outside of the CMA9 mandate".* As they are outside the Standard there is a high degree of variability. Some "*PISPs … have begun to offer solutions to the lack of standardisation*". In the view of this submission, "*Standards could be developed rapidly with industry collaboration."*

### Potential Areas of Alignment

It is clear there is limited alignment in this area, with ASPSPs suggesting that this is not a priority area for improvement, or at least not without the ability to drive commercial returns. One submission suggests that a number of banks are already innovating in this space outside the Open Banking Standard, which provides a more nuanced view of both the opportunity and banks' preparedness to invest under the right commercial conditions.

It was, however, clear that we lacked expert input on this topic, with many responses having limited experience and providing no response or a very limited one. It may be advisable for the Committee to engage SME payment experts before drawing firm conclusions on the potential in this space.

### 1.20.3. Section 3: What are the longer-term changes?

#### *1.20.3.1. QUESTION 3.1 Transaction Risk Indicators (TRIs)*

***We have asked the Data Sprint to consider fraud data sharing and TRIs, costs and benefits associated with adopting these solutions and the specific data field that would be needed to be shared. Are there specific elements in relation to payments that you would like to highlight?***

**Areas of Discussion**

There was near-unanimous agreement that implementation of TRIs was a **key short-term priority** that would provide significant anti-fraud and false-positive reduction benefits. Respondents were generally supportive of the work previously undertaken by the OBIE in this area and considered that the key need was for this to be consistently implemented. However, one TPP suggest that further work to empirically evaluate the fraud risks associated with open banking transactions should be undertaken first.

Most respondents were broadly satisfied that the data fields introduced in the latest version of the Open Banking Standard – 3.1.10 – were a good starting point, and that consideration of other data elements should be deferred until these were sufficiently embedded within the market and their effectiveness assessed. It was widely acknowledged that TRIs would need to evolve as their efficacy was measured and in response to emerging fraud risks. Some TPPs suggested that a few core TRIs should be implemented, and their effectiveness assessed, before mandating a more expansive set of options in the current Standard that relied on more complex definitions (e.g., payment purpose codes). However, banks generally saw significant benefit in receiving enhanced data on the nature of the underlying payment. One TPP proposed extending the existing payment purpose code list to include a new data element “Cash Withdrawal” or “Transfer”, to support a cash withdrawal use-case. Reference was made by some respondents to the need to provide PSU names and account type in a standardised format.

Respondents universally agreed that to realise the benefits of TRIs, PISPs need to provide accurate data, followed by banks using this data to risk-assess the transaction. Some respondents, principally banks, suggested that this can only be achieved through central monitoring and enforcement of adherence to standards by both TPPs and ASPSPs. Some TPPs agreed with this proposed approach, but a majority suggested that a managed roll out of TRIs by the OBIE or a Future Entity would be sufficient to achieve the shared objectives of all participants.

A number of respondents referenced the new cross-industry Enhanced Fraud Data Standards and processes that are currently being developed. There was a desire to see delivery of this initiative prioritised, and consideration given to how it could best support open banking payments.

### *1.20.3.2. QUESTION 3.2 Multilateral Agreements*

***We have asked the ecosystem sprint to consider MLAs and the different options proposed by members. Is there anything different, specific, more urgent for payments that you would like to emphasise? And what is the key payment use-case that should be prioritised? For example, should non-sweeping VRPs be the initial focus?***

#### Areas of Discussion

Some TPPs considered that the case for MLAs has not yet been made and that it was important to first identify what problems need to be addressed. It was generally agreed that MLAs would be considerably more effective than trying to set up a portfolio of bilateral agreements. A platform suggested that it is too early to determine whether MLAs are necessary and recommended evaluating how the market evolves using bilateral agreements, before embarking on the more significant task of building and negotiating MLAs, as it could delay market development. Most TPPs concluded that MLAs should be thin and only resolve specifically identified gaps in particular use-cases.

Most TPPs stated that an initial focus should be on the development of a multilateral framework for non-sweeping VRPs, but a few recommended an extension to include payment initiation regardless of whether it is VRPs, PIS or Request to Pay. One TPP stated that it could be difficult to achieve agreement on MLAs in relation to VRPs given the more complex risk and liability issues arising from the absence of SCA. However, some banks did not consider non-sweeping VRPs to be a priority use-case, and suggested instead that the key area of focus should be on other A2ART use-cases.

Some banks agreed that key issues identified in the interim report, e.g., commercial / remuneration model, liability model, dispute resolution roles and responsibilities, and operational service level agreements could usefully be addressed by MLAs. One bank indicated that a scheme approach might be a more appropriate approach to achieve this rather than MLAs.

Consumer experts raised concerns that industry-agreed MLAs might not satisfactorily deliver key essential elements e.g., sufficient consumer protection, since there might be limited market incentives. Their preference is for a regulator-led solution, with the regulator(s) consulting on the design of an open banking payments scheme which reflects the needs of end users. This would ensure that appropriate consumer protection measures, including appropriate levels of redress, are built in from the outset.

One platform provider argued that Pay.UK should have responsibility for extending the rules and standards for FPS so that PISPs to join an enhanced FPS scheme.

### *1.20.3.3. QUESTION 3.3: Liability*

***Where should liability for the different types of dispute lie (banks, TPPs, merchants or consumers, a mix)?***

- **a) Bankruptcy protection**
- **b) Breaching sales contract (e.g., goods not received, or not as described)**
- **c) Fraudulent merchant**
- **d) Other (please give examples)**

#### Areas of Discussion

Many respondents noted that this was a complex issue which requires detailed evaluation. Several respondents urged the Committee to allow this question to be explored in more detail and convene a cross-industry working group to achieve this.

Many banks argued that liability should not invariably reside exclusively with the banks as this may act as a potential barrier to the expansion of open banking payments. However, some of them recognised that allocating a share of liability to TPPs could be a barrier to entry to the PISP market, as PISPs are unlikely to have the funds to absorb significant fraud losses and in many circumstances are not in the flow of funds, so cannot use merchant receipts as a form of collateral, similar to card acquirers. However, banks were of the view that a future liability model should make sure that all PISPs are responsible for undertaking appropriate fraud checks.

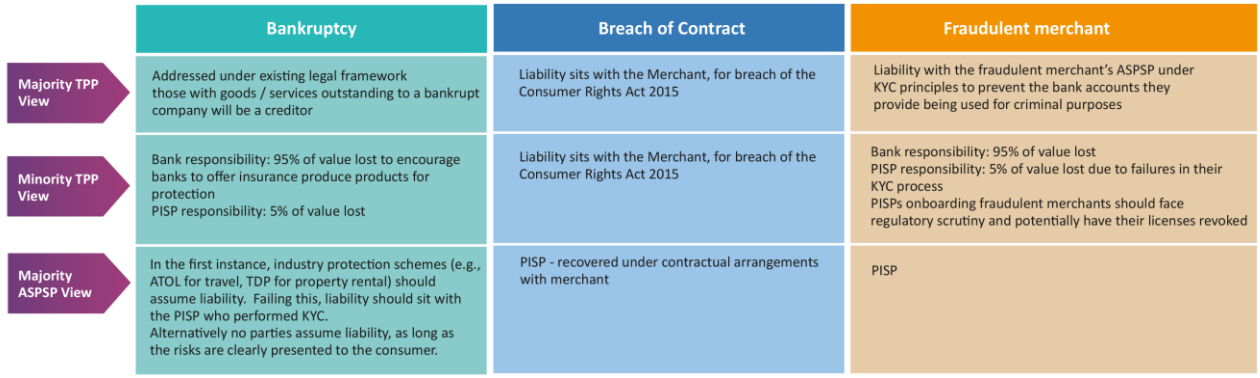
Most TPPs noted that consumers in the UK are covered under the Consumer Rights Act 2015 for products that are not as described, fit for purpose or of satisfactory quality, regardless of payment method, and that there were established mechanisms for claims to be made. For certain transactions, consumers benefit additionally from industry schemes such as the ATOL and ABTA travel schemes. In cases where consumer detriment arises from payments being made to a fraudulent merchant, the majority of TPPs argued that liability should reside with the merchant's ASPSP. Their view was that the merchant's ASPSP has a responsibility to KYC their customers (and their business) and is therefore in the best position to identify and stop receiving accounts being used for criminal purposes.

Consumer experts strongly argued that there must be effective mechanisms in place to address circumstances where the merchant fails to provide the good or service ordered, and that they need certainty about how such disputes will be handled, including an independent body to adjudicate where necessary. Their view was that: "*It is unconscionable for consumers to be held liable for disputes relating to bankruptcy, a breach of a sales contract, or a fraudulent merchant. Consumers need to be protected – they cannot be expected to undertake due diligence about the robustness of a firm's financial position, or to undertake extensive investigations into a merchant to ascertain whether they may be fraudulent before making a payment.*"

They argued that close attention should be paid to existing dispute management models deployed by other payment methods (e.g., chargeback for debit cards, section 75 protection for credit cards, guarantee for Direct Debits), since they have delivered reasonably strong consumer protections.

A summary of where respondents felt that liability should best reside is set out in figure 9 below.

***Figure 9 – Perspectives on where liability should reside.***




## 1.20.4. Section 4: Which actor(s), including the Future Entity, should play a role in operationalising the items outlined (in Sections 1-3)?

***QUESTION 4.1***

***What is the role of the Future Entity in supporting ongoing evidence collection (outlined in section 1) and the delivery of any of the changes highlighted under the short term and long-term categories (sections 2 & 3)?***

***QUESTION 4.2***

***What is the role of Pay.UK in supporting the delivery of these changes, i.e., are changes to the clearing and settlement infrastructure required?***

***QUESTION 4.3***

***What are the roles of industry and regulators in operationalising evidence collection and the delivery of the proposed solutions for payments?***

***QUESTION 4.4***

***What is the role regulators should play? Where is regulatory intervention required and what type of intervention is required?***

### *1.20.4.1. Areas of Discussion*

#### Area of Discussion 1: Data collection

There was a broadly held, but not universal view that the Future Entity should have an important role in the collection of data and evidence to support open banking. Examples of data that the Future Entity could collect were API performance, fraud levels and types, and legitimate transactions declined. Nine TPPs, two expert advisers, one platform and one ASPSP specifically recommended that the Future Entity needed to play an important role in collecting data from across the open banking ecosystem.

A number of respondents felt that this role would benefit from regulatory support or direction, that would ensure that the Future Entity had the powers to require this information from a wider range of participants and provide a broader base of MI than the OBIE currently has.

However, one ASPSP felt that if the Future Entity were responsible for data collection, this may create duplication, and a more efficient method would be for the FCA and the PSR to augment their existing data collection requirements. This idea appeared to be supported by a TPP in the discussion meeting, but the TPP also provided evidence calling for the Future Entity to have a role in data collection. Another ASPSP felt that there was already extensive reporting of performance data to the OBIE and warned of *"diminishing marginal returns in building ecosystem data infrastructure"*.

### Area of Discussion 2: Enforcement of delivery and standards

Whilst there appeared to be broad agreement that the Future Entity should have a role in the development of Standards, there was a range of views regarding its potential role in the enforcement of those Standards or delivery of a future roadmap.

*"[The role of the Future Entity includes] ensuring there is full compliance with the current mandatory standards under the CMA Order, and the best possible version of them rather than the 'bare minimum' … delivering changes in line with a clear, UK open banking roadmap."* – TPP one

*"The Future Entity should also be empowered beyond the CMA9, as [there are] a number of the 'inconsistencies' in API performance and service coverage"* – TPP 2

*"The role of the Future Entity should be limited to that of a standards body."* – ASPSP

### Area of Discussion 3: Development of MLAs

Four TPPs and one ASPSP identified that the Future Entity should play a role in the development of multilateral frameworks:

*"Monitoring the fairness and efficacy of any multilateral framework that is defined (e.g., for non-sweeping VRPs."* - TPP

However, others felt that direct regulatory intervention would be required to address the challenge of misaligned incentives or to ensure that appropriate consumer protection is delivered:

*"The regulator role will be to ensure they mandate appropriately."* – TPP

*"[A regulator is needed for] supporting the creation of cross-market incentives [and] commercial models to help delivery of any proposed solutions for payments"* – ASPSP

*"Regulatory intervention is required [for setting up] conduct and liability frameworks."* – Expert adviser

### Area of Discussion 4: Role of pay.uk in the ongoing development of open banking

There was a divergence of opinion regarding the appropriate role Pay.UK should play in the future development of open banking. Generally, most respondents favoured a limited Pay.UK role with responsibility shared between the Future Entity and regulators. TPPs and some ASPSPs felt that Pay.UK should focus on the existing payment system, critical national infrastructure and the development of the NPA, and that a separate Future Entity should develop the Open Banking Standards. One TPP identified that a formal memorandum of understanding between the Future Entity and Pay.UK could be an effective way to bridge the two organisations. Another TPP went

further, recommending that all overlay services, including open banking, on the payment rails should be the responsibility of the Future Entity.

One platform provider felt that, if required, Pay.UK could augment its capacity and capability to deliver an expanded remit. A minority of ASPSPs identified that there may be cost efficiencies if the activities of the Future Entity were combined with Pay.UK.

One TPP raised concerns over Mastercard's ownership of Vocalink, as Mastercard is the infrastructure provider for a card payment system and the inter-bank payment system. It notes that the development of A2A and open banking payments is intended to provide a credible alternative to card payments and increase competition between payment systems. Their view is a conflict of interest could arise if Vocalink were selected to provide the supporting infrastructure for NPA and is involved in decision-making over the governance and design of the NPA.

### Area of Discussion 5: Regulatory intervention

Another area where there was a divergence of opinion was around the level of regulatory intervention required to support the continued development of open banking:

- TPPs demonstrated more appetite for regulatory intervention and cited a number of specific areas including:

  **Data Collection:** Several TPPs cited that regulators may need to define the data being collected, or provide the Future Entity with the authority to collect data from participants to ensure the "efficient and fair operation of Retail and SME payments".

  **VRPs for Non-Sweeping:** Several TPPs indicated that regulatory intervention would be required to ensure availability and access to VRPs for non-sweeping use cases. Concerns were raised that this capability would not be quickly brought to market without regulatory intervention, particularly because the platform nature of payments means that nearly all of market coverage is required before a viable service can be developed.

  **Multilateral Arrangements:** As mentioned earlier there was fairly widespread support for regulatory intervention to support the development of MLAs, and respondents suggested a level of intervention ranging from approving proposed MLAs, tasking the Future Entity to develop MLAs or directly intervening on pricing for access (for example, for VRPs).

  **Conformance:** Many TPPs felt that regulators needed to ensure all open banking participants built high quality APIs and ensured consistent standards across ASPSPs. One respondent suggested fines or public naming might provide appropriate incentives, others suggested that the Future Entity be empowered to investigate on regulators' behalf and work with participants.
- One platform recommended that the regulatory intervention should be minimised to allow the industry to develop the market, and one ASPSP felt that the first step for development *"should start with seeking to outline a broad vision of what the industry (including the wider 'ecosystem') wants to achieve for Account-to-Account payments".*
- One platform and one ASPSP suggested that the regulator needs to define what the role of the Future Entity should be and provide it with the appropriate remit.

- One ASPSP felt that it would not be possible to hold a definitive view of the role of regulators until the roles of participants and the vision were clear, but they were not opposed to the Future Entity gathering evidence.

#### *1.20.4.2. Emerging Areas of Agreement*

There were two topics where there appeared to be alignment among respondents:

**Ongoing development of the Open Banking Standard**. Any standard needs to be maintained and almost all respondents felt that this should be a role of the Future Entity. Where there were differences of views was regarding whether that role should be extended beyond the Open Banking Standard to support other standards such as open finance.

**Collaboration between the Future Entity and Pay.UK.** All respondents who commented felt that it was important that the NPA was developed with open banking in mind so that there would be no unnecessary rework. Similarly, it was mentioned that the NPA may be able to address some of the challenges in open banking payments, particularly the development of now or never payments, where the payment initiation is accepted only if the payment will be made, so transactions never have a pending status. For these reasons there was widespread support for the collaboration between the Future Entity and Pay.UK. However, the majority view was that Pay.UK should have a limited role.

### 1.20.5. Priorities

***QUESTION 4.5***

***What in your view are the top three short term priorities and top three longer term priorities to be addressed in a roadmap for the future development of open banking+ payments? What would be reasonable timeframes for these to be achieved?***

Respondents gave evidence on their priorities. The different priorities have been clustered into priority themes and are summarised in the figure 10 below:

***Figure 10. Key Priorities: Payments***


- Optimising the Open Banking Standard and ensuring widespread standardised adoption was seen as the highest priority. This category includes improving the operational performance of the system leading to improved customer experience (e.g., higher consent rates and better information when journeys do not complete).
- Another key priority is getting the right balance between fraud and friction to ensure ASPSP interventions are targeted at higher risk transactions.
- Long-term payments strategy is a very broad theme and includes open finance and open data, and alignment of open banking payments to the NPA initiative.
- TPPs place significantly higher priority on non-sweeping VRPs than banks and other respondents.
- On the other hand, banks and other respondents placed higher priority than TPPs on setting up a robust and enduring customer protection mechanism.

## 1.21. Second Data Strategy Sprint

### 1.21.1. Section 1: What do we need more evidence on?

#### *1.21.1.1. QUESTION 1.1: Fraud Data*

***Statistics in relation to attempted and successful fraud cases of open banking payments against other direct banking channels and granular data on the frequency, types, value, use cases of attempted fraud, successful fraud and "false positives" cases of open banking payments.***

- ***What are the key metrics TPPs and ASPSPs should provide data on to enable JROC to have a view on current levels of fraud? Please share case studies of attempted and successful fraud cases that highlight key system vulnerabilities.***
- ***How should data collection be operationalised, including who should take this forward, in the short-term and on an ongoing basis as open banking+ develops?***
- ***Should this insight be shared across ecosystem and what is the best way to do this?***

**Areas of Discussion**

**Area of Discussion 1: Key Metrics**

The importance of having comprehensive data and robust mechanisms to monitor the incidences of fraud was widely acknowledged across all participants. It was also noted that, as fraud vectors change, existing metrics will need to be adapted.

Key suggested metrics included:

- **Volume/value of losses categorised by fraud/ scam type.**
- **Volume and value of attempted fraud incidents by fraud/ scam type.**
- **Volume and value of prevented fraudulent transactions by fraud/ scam type.**
- **Volume/value of losses and attempted fraud by use case / payment type.**
- **Gross and net fraud losses categorised by fraud/ scam type.**
- **False positive statistics.**
- **Completed successful transactions.**
- **Comparative fraud data of attempted and successful fraud cases of Open Banking payments against other direct banking channels.**

**Area of Discussion 2: Data Collection & Sharing**

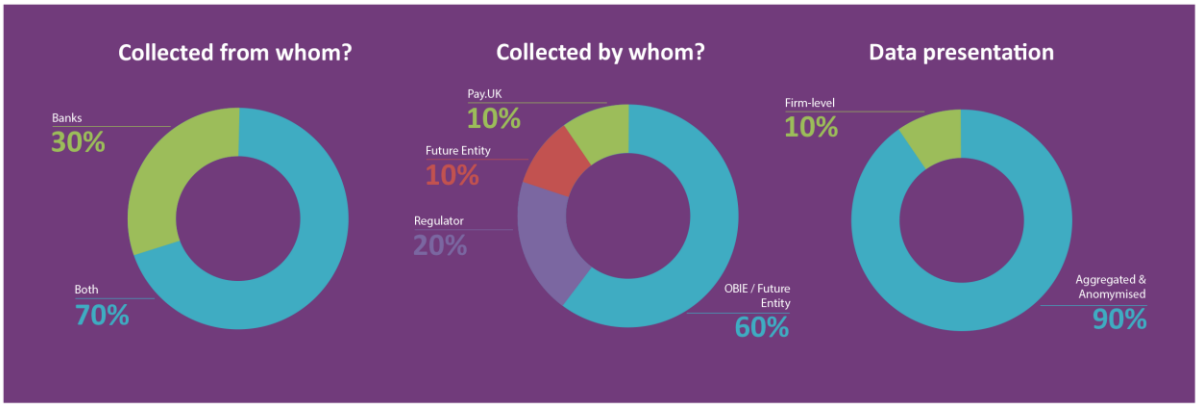
Most respondents suggested that data should be collected from and shared between both ASPSPs and TPPs to build a comprehensive view of fraud. However, a minority of respondents recommended that data should be supplied exclusively by ASPSPs on the basis that they are the party applying transaction monitoring, the first point of contact for customers, and are well placed to provide information on attempted fraud, deferral and rejection rates by channel. Most respondents considered that the OBIE should commence this activity prior to the Future Entity being established.

Most respondents also saw the Future Entity as having the primary responsibility for collation of cross-industry open banking fraud statistics. They also recommended that, to avoid duplication, when considering any new data requirements, opportunities should be taken to align with existing reporting mechanisms.

Other views highlighted that fraud data is already collated by UK Finance and is also supplied to the FCA under REP017 reporting obligations and these mechanisms should be used. Similarly, some respondents referred to the current PSR consultation on APP fraud and recommended alignment with its proposals for the collection and publication of APP fraud data. A few respondents considered that given these arrangements, UK Finance, regulators or Pay.UK should play an extensive role in data collection.

The range of views on which parties should supply data and the entity that should have responsibility for collecting it as set out in figure 11 below.

***Figure 11. Data supply and entity responsible***




An overwhelming majority (90%) of respondents agreed that anonymised data should be submitted to enable trends to be analysed and shared with ecosystem participants. The primary reason for this approach is to ensure that data cannot be exploited by criminals as they seek points of vulnerability. It was also noted that sharing with non-regulated parties poses increasing risks of wrong interpretation and reputational damage.

Additionally, some TPPs recommended that a fraud forum is convened by the OBIE and/or Future Entity to enable the exchange of emerging threat information and discuss any concerns.

## 1.21.2. Section 2: What can we do in the short-term?

### *1.21.2.1. QUESTION 2.1: Role of Customer Attribute Data in Risk Management*

***In the first sprint, many TPPs identified a number of additional customer attribute data that would improve their own risk scoring. However, some TPPs and all the banks questioned whether TPPs can realistically play a key role in fraud detection given the disparity in the information available to them. What are the pros and cons of providing additional identify-related information to TPPs? Would the Standards need to be updated and what is the implication on timelines?***

Several respondents suggested that it would be beneficial to convene workshops to explore what data TPPs believe would be helpful for ASPSPs to provide and for what purpose. Banks generally noted that in conjunction with this there is a need to review whether shifting some liability to TPPs provides appropriate incentives for ASPSP to share a wider range of data with TPPs. Some respondents also called for regulators to work with stakeholders across the public and private sector to meaningfully contribute to a public-private strategy for tackling fraud.

#### Areas of Discussion

#### The Advantages

A TPP noted that open banking attribute data could be used to prevent fraud beyond payments. It has potential to prevent identity theft in credit applications where fraudsters use a victim's credit bureau record to apply for credit, while supplying their own bank details to receive loan proceeds. Fraud is also perpetrated by using fraudulent card details from which loan repayments are taken.

The TPP currently manages this risk by using account name data accessible by AIS in order to match this with credit bureau data. The second risk is mitigated by attempting to identify whether the card on file is linked to the bank account from which AIS data has been shared. However, they noted several current barriers to achieving this:

- Name matching is imperfect as names are not unique, nor immutable.
- The quality of the data varies across different ASPSPs.
- In some cases, this data is available but only via premium APIs.
- Only a few banks (and only one of the CMA9) were reported to provide the four digits of the card associated with the account, which is an optional but valuable field within the Standard.

TPPs were clear that improving the availability of optional data fields, including address and date of birth and partial card number data, would be beneficial. Consistency in the account holder data was raised by several TPPs, noting that some ASPSPs do provide robust name of account information, and others do not. This is particularly challenging in relation to business accounts.

TPPs also noted that they often have deeper data sets, which could be leveraged by banks to reduce the number of false positives where legitimate open banking payments are blocked.

#### The Disadvantages

Expert advisers noted that attribute data, while of utility for fraud prevention purposes, can also be used to exclude less profitable customers. It is important to properly define that shared data will only be used for the former purpose. They also noted the unintended risks of being flagged as higher risk where the relevant identity related data was unavailable. They also expressed concern regarding

the potential accuracy and validity of attribute data, for example date of birth, noting that there were a variety of ways in which the data may have been originally obtained and the extent to which it may have been self-asserted rather than independently validated.

A trade association also highlighted the complexity of addressing issues of liability when participants relay on data which proves to be inaccurate.

Some banks questioned whether in the short-term it would be more expedient to focus on data sharing between payer and payee ASPSP, given a proof-of-concept evaluation that shows this to be effective. They also noted that a key intentional design feature of open banking is the low-cost, low-information model, predicated on not sharing payer information with the TPP. Sharing of additional customer attribute data would represent a significant shift in direction requiring development of rules, contracts and commercial models.

It was noted that an Extended Customer Attribute standard already exists as a 'premium' API but has not been implemented by ASPSPs as commercial and liability models are unclear.

One bank, while welcoming appetite to reduce fraud at any stage of an attempted payment, questioned whether it is feasible for TPPs to manage fraud effectively using technical solutions and set out several concerns that the blurring lines of accountability for fraud management would present several challenges, notably:

| | |
|---|---|
| **Customer Experience** | a) Customer clarity is needed as to who has blocked a payment, who to contact in such an event and where to report suspected fraud. ASPSPs have established systems and processes to achieve this. Altering these would be counterproductive.<br>b) Would additional friction ahead of the authentication step introduce unhelpful friction in payment journeys. |
| **Efficacy** | • **ASPSPs' fraud models use mechanisms such as device identification, location, spending patterns. These mechanisms are best supported at ASPSPs where the end-customers' entire payment behaviour is observable.** |
| **Consent** | • **Any sharing of customer attribute data risks would require customer consent, further increasing friction and potentially conflicting with data minimisation requirements.** |

### *1.21.2.2. QUESTION 2.2 Transaction Risk Indicators*

***a) What are the barriers to the consistent adoption of TRIs by all?***

***b) What is needed to remove those blockers?***

***c) What are the costs for ecosystem participants and the time needed for implementation?***

***d) Should there be a regulatory requirement to use TRIs? Could a similar approach to the RTS Transaction Risk Analysis exemption (based on actual fraud thresholds) be used?***

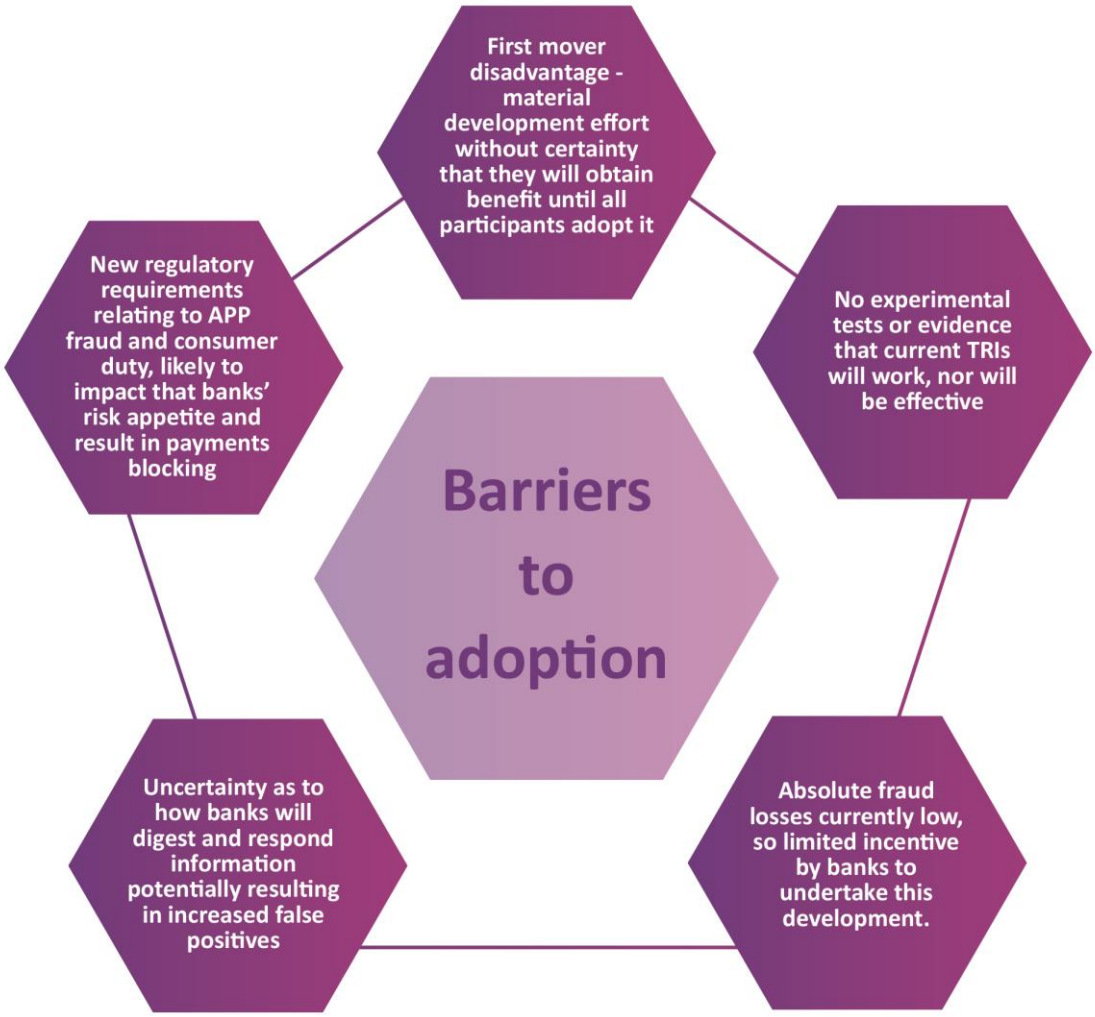
#### Areas of Discussion

#### Barriers to Adoption

The majority of respondents indicated that development of the Standards covering TRIs was a welcome development given the likely progression of open banking payments to support an ever-greater number of merchant commerce use cases.

However, it was evident from responses that although new TRI requirements have been introduced into the latest release of the Open Banking Standard, and despite a universal acceptance that they were of utility in identifying fraud, few firms had implemented them. Expert advisers noted that there are significant risks for the whole ecosystem associated with piecemeal adoption of risk indicators. There is also a risk of arbitrage where some institutions, with different risk appetites, respond differently to the risk indicators (if received) or may even choose not to use them at all.

***Figure 12. Barriers to Adoption***




The primary barriers to adoption identified by respondents are set out in the figure below. The most consistently referenced barrier was first mover disadvantage. It was noted that the development requirements to enable TPPs to supply the data and for banks to utilise it in their risk scoring engines is material. Any party (be it ASPSP or TPP) that makes the investment in building TRI capability will have invested time and effort in a technology but cannot realise benefits until all the other ecosystem participants also adopt it.

As it stands, there is no mandatory requirement on TPPs to provide TRIs or for ASPSPs to make use of the information when provided. The only current requirement on the CMA9 is to be able to receive TRI data.

### Overcoming these barriers

There was broad agreement that some actions are necessary to overcome the first mover disadvantage issue described in the preceding section. However, there were divergent views as how

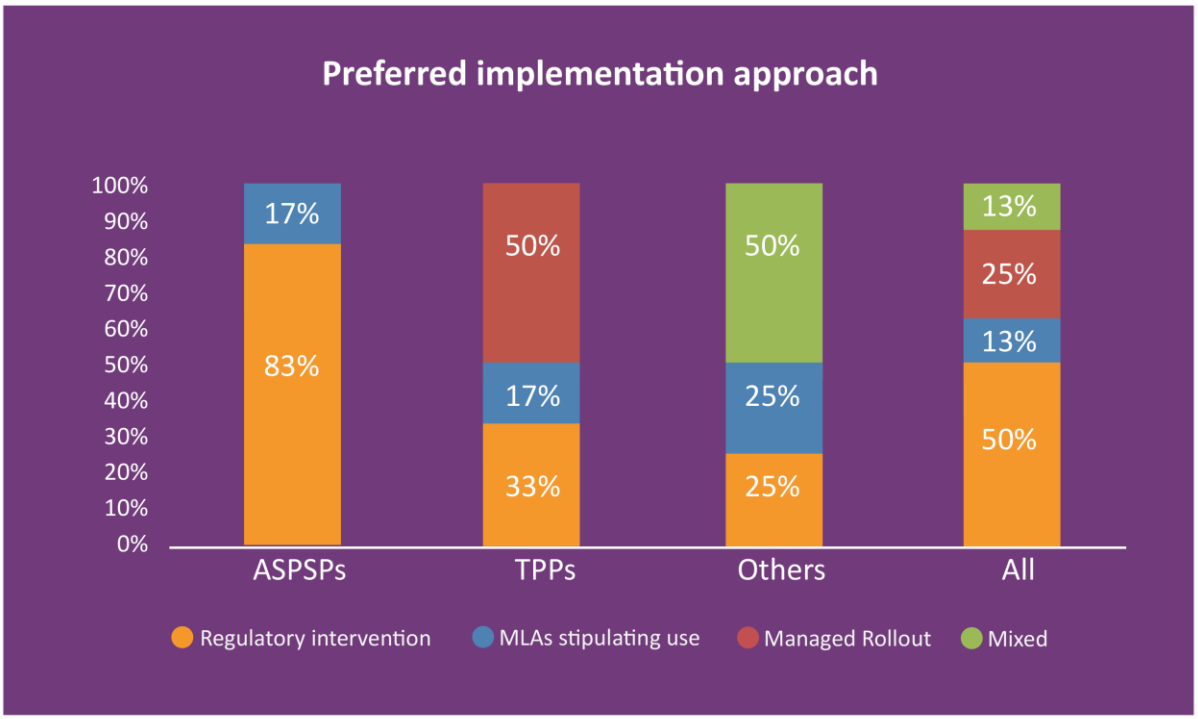
best to achieve this. The majority of respondents believe that regulatory intervention is required to make use of TRIs obligatory across the entire ecosystem. TPPs would therefore be required to provide TRI data and all ASPSPs, including those beyond the CMA9 compelled to use them. It was noted that this would require compliance monitoring to ensure that not only that all parties were supplying the required data, but also that it was of a satisfactory quality and being appropriately used.

Some respondents indicated that an alternative to regulatory intervention might be achieved through the use of MLAs that would require all participants to adhere to an agreed set of rules. It was, however, noted that this would only achieve the intended objective if a sufficient number of market participants voluntarily agreed to use MLAs.

Other respondents proposed that adopting a managed roll-out of TRIs including guidance covering not only a recommended approach to implementing TRIs but also principles that harmonise how banks respond to TRIs, with an emphasis on preventing inadvertent outcomes, e.g., banks applying blanket blocks to certain categories of payments. It was felt that this approach would provide participants with sufficient confidence to make investment in the delivery of TRIs, resolving the "chicken and egg" issue that is currently preventing widespread adoption of TRIs.

One bank suggested that it would be helpful to pilot TRIs for six months to enable ASPSPs to refine their risk scoring approaches data collection and analysis so they can respond to TPP concerns before being using TRIs actively. The proportion of respondents favouring each approach is set out below. (Note: some trade associations which responded indicated that their members had conflicting views – these have been categorised as mixed.)

***Figure 13. Preferred implementation approach for multilateral agreements***




### Implementation Considerations

A number of TPPs indicated that it might be useful to prioritise the implementation of certain TRIs for the highest priority use cases (e.g., payments for utilities, HMRC etc), which are broadly considered low risk.

One TPP suggested that giving banks reasonable confidence in the legitimacy of the payee could play a significant role in establishing that a transaction is low risk from an APP fraud perspective. They suggested that consideration is given to establishing a comprehensive database of "known legitimate payees" (or whitelisting), which might initially include HMRC and other Government and local authority accounts. This respondent also noted that a key component of the existing TRIs is the extent to which a payee is "known" to the TPP. They considered that it would be helpful to provide more granular information via TRIs as to how this validation had been achieved and notably whether:

1. **The payee has been onboarded by the TPP via AIS.**
2. **The payee has been onboarded via an "offline" KYC process.**
3. **Both of the above.**
4. **The payee has not been onboarded.**

Another TPP considered that it would be beneficial to extend TRIs to include behavioural risk TRIs, which would have an upside to reduce payments fraud.

### RTS Transaction Risk Analysis Exemption

The RTS Transaction Risk Analysis Exemption enables merchant acquirers to choose to apply an SCA exemption flag if fraud rates are below a reference rate. The responses to this question were inconclusive as respondents had different interpretations on how a similar exemption might apply in open banking.

Several banks agreed that employing a regulatory mandate similar to that for the Transaction Risk Analysis exemption would have some merits, given that it would be highly enforceable and ensure that the burden of providing TRI data is focused on those participants with high fraud rates.

A few TPPs agreed that it would be useful if this approach required banks to increase their transaction limits and reduce interventions for transactions originating from PISPs that have low fraud rates. It was noted, however, that this would require an independent arbiter of fraud rates and a clearer definition of what constitutes fraud in a PISP transaction.

However, other respondents noted that the reason Transaction Risk Analysis exemption operated effectively in the card payment market was because card schemes provide rich and comprehensive risk scoring data for every merchant, using network level data on the number of chargebacks submitted against that merchant. The absence of comparable data in an open banking context led some respondents to conclude that this is not a viable solution.

### *1.21.2.3. QUESTION 2.3: Propositions for consumers in vulnerable circumstances*

***How can regulators better support the development of propositions that benefit consumers in vulnerable circumstances, promote financial inclusion and ESG? For example, should there be more targeted support from the FCA's Innovation Pathways or use of the sandbox?***

#### Areas of Discussion

There were divergent views as to whether this was an area where regulators should intervene. Two responses, one from an ASPSP and one from a TPP, felt that this shouldn't be a priority area. "*The market is already solving this"* was one comment. In a similar vein the other noted that, "*Regulators should not be required to support the development of propositions as this should be allowed to develop in the market."*

These were minority views, however, with all other responses identifying a range of areas in which regulators could act, albeit with very little agreement in terms of what type of activity was needed. Key themes which emerged from the evidence are outlined below.

#### Research with people with lived experience of vulnerability

The first theme was insight into consumers in vulnerable circumstances. Three submissions felt that we have insufficient insight today and regulators should work with charities and other experts to undertake research with consumers with lived experience of vulnerability. A typical quote was: "*Regulators and the OBIE should create a fund for consumer research and enable consumer organisations to submit proposals for research. This would enable the best ideas to be funded and ensure a clear voice for consumers, particularly vulnerable consumers and those from excluded communities."* This was echoed in a submission from Sprint 1 from an expert adviser who was not able to provide a submission to Sprint 2.

One submission went further and suggested that regulators should set up an expert reference group: "*The regulator, industry bodies and the financial services industry could work together in setting up and managing an expert reference group to specifically design services that support customers and SMEs through the cost-of-living crisis."*

#### Explore and understand why propositions are withdrawn or not brought to market

Three submissions highlighted the issue of commercial viability in regard to services targeting this consumer group: "*Solutions offering more novel support to people in vulnerable circumstances are typically small and have yet to scale consistently."* Other submissions went further, highlighting two services that have left the market: one targeted consumers with mental health conditions and the other older consumers. One submission highlighted that, *"Some socially important use cases may not generate the necessary revenues or commercial outcomes necessary for the business to reach sustainability. Several propositions have exited the market already. Regulators may need to assess social impact and intervene in these situations to mandate cooperation of participants and enforce cost measures to enable such use cases to exist."*

#### Exploring new propositions to support vulnerable customers

The suggestion of using FCA sandboxes was supported by four responses and was not considered to be a particularly radical step.

Four submissions suggested that broadening data sets would be particularly valuable to supporting vulnerable customers, by providing a broader overview of their financial situation. One independent

expert cited experience from the responsible credit market where having API access would help significantly in the ability to provide refinancing loans to customers. At present, it is very hard for lenders to be certain that funds are actually being used to pay off other loans held. This creates significant risk and, in some cases, reduces the amount that the lender is prepared to lend.

One submission from a TPP provided evidence about additional data that would enable them to identify categories of vulnerability more accurately. These included:

- **time stamps of transactions**
- **full PoS data for card transactions**
- **joint account flag and,**
- **additional data on inbound and outbound transactions.**

Already, this TPP has been able to identify "destructive financial behaviours" in around 10% of loan applications, which could be effectively identified through open banking data. The additional data could help identify vulnerable customers even more clearly.

Beyond this, there were some individual responses, but these were isolated and did not feature in other submissions. These included accelerating agent registrations, which are acting to slow services coming to market, blocking gambling payments when customers use open banking payments and sharing vulnerability indicators across the market (with consent).

#### Potential Areas of Alignment

As the above analysis demonstrates, there was alignment that regulators should do more to support the emergence and scaling of services targeting consumers in vulnerable circumstances, but little commonality into how. The most widely cited interventions were in the areas of research and understanding the commercial case of such services. There were clear connections to other areas of evidence however such as expanding to new data sets.

### *1.21.2.4. QUESTION 2.4: Extending Access to New Data Sources*

***A respondent mentioned the benefits of being able to access data from sources such as NS&I to open banking. Are there other example sources which should be considered? What is needed for this to happen?***

#### Areas of Discussion

#### New Data Sources

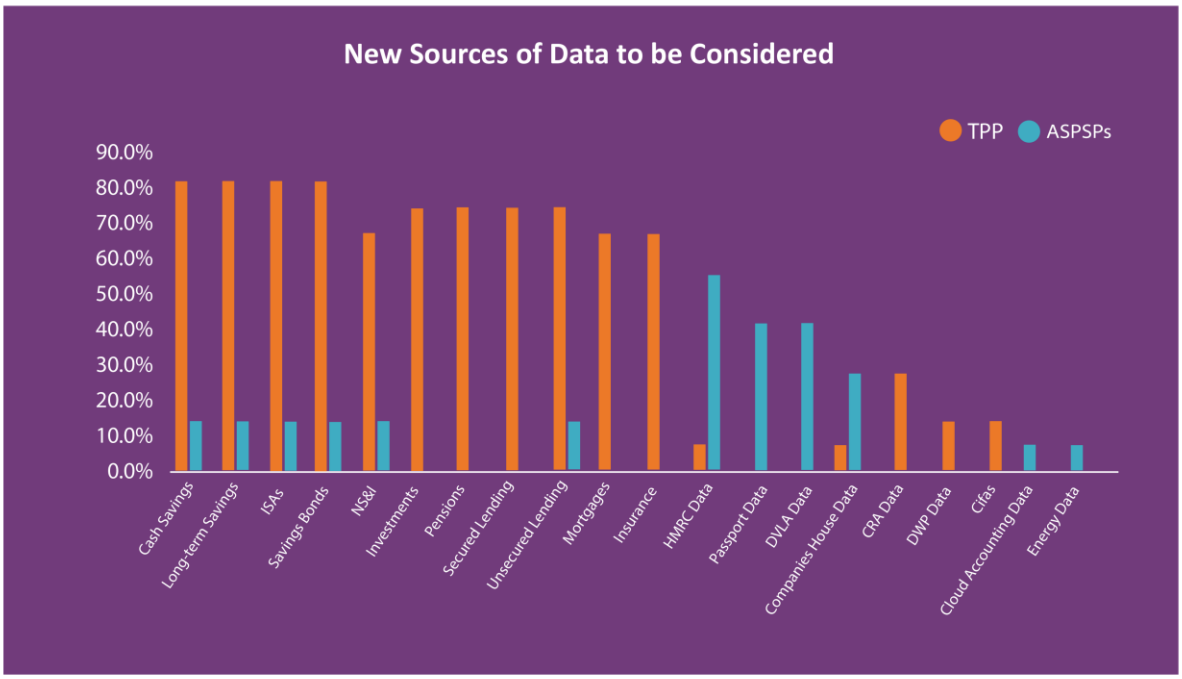
There was universal agreement that open banking propositions will benefit from increasing scope and availability of new data sets. However, there were clear differences between banks and TPPs as to the nature of those data sets as summarised in the graph below.

In TPP responses the focus was predominantly on expansion initially into adjacent financial products, including savings and investments, which would provide TPPs with a holistic view of a consumer's financial situation. This would increase the effectiveness and positive impact of the customer-facing products drawing on these feeds, for example personal finance or business dashboards helping people and SMEs better understand their financial position and to make better, more informed decisions as a result.

Banks, on the other hand, identified access to sources of government-held identity attributes as more important. This information could be used to improve onboarding, verify identity and reduce fraud.

Several banks stated that they were unclear as to the purpose of expansion of open banking into savings accounts, or under what remit and governance it would proceed. They questioned, on the basis of their experience in relation to open banking, whether regulator-led initiatives can deliver benefits that justify the costs. In their view, any such proposed expansion should be predicated on a clear problem statement, an assessment of market ability and willingness to meet the need and a strong cost benefit analysis.

***Figure 14. New data sets for consideration***




The starting position for most TPPs is that all end user-owned data needs to be sharable via APIs with regulated third parties. They noted that most ASPSPs already have APIs built to support access to savings account data, all they would need to do is open these up to TPPs. The current 'payment account' definition prevents access to numerous providers and accounts. Indeed, some ASPSPs prevent access to certain savings products because of the regulatory definition.

Expert advisers highlighted the potential competition benefits of opening up access to savings, with significant inert balances: "*A conservative estimate of the benefit available to consumers… would be over £3.8 billion a year*." They were also keen to see how, for retirement savings, the Pensions Dashboard initiative will open up new opportunities to introduce new data opportunities.

### Access to APIs

Some TPPs noted that the savings market was vibrant and that new entrants had recently entered the market. A view was expressed by several TPPs that there have been a number of new entrants to the UK current account and savings market recently, and it is therefore a valid question to consider

how long such players would be given to open up API access after they launch. For some TPPs, it was unacceptable for new entrants to enter the UK market, take a considerable market share, and not support open banking. However, another submission suggested a threshold should be agreed for new entrants, at which point they must open up API access.

#### *1.21.2.5. QUESTION 2.5: Credit decisioning*

***Other respondents indicated that open banking data in other jurisdictions has emerged as an effective and scalable use case to support credit decisioning/lending, particularly for SMEs? What more is required to expand usage of open banking data in this space in the short term?***

**Areas of Discussion**

**The Opportunity**

Expert advisers noted that open banking data could provide additional data for scoring purposes, opening access to credit for less "traditional" customers who may not have extensive credit histories (similar to the use of a history of regular rental payments alongside mortgage payments to support mortgage applications). It was noted that there is a real risk that the existing credit reference agencies continue to dominate this market, simply adding the extraction and analysis of open banking data to their existing products rather than introducing new competition.

In the small business sector, it was noted that there are around 4.9 million micro businesses in the UK (fewer than 10 employees). Open banking is rarely used in business lending and many business lenders are still not clear or convinced that pre-approvals work. This is a clear opportunity.

It was also noted that while some consumers will benefit from the extension of available data that enables 'fairer' consideration of their actual circumstances, there is a danger that this data can be used against them. Examples provided were that a lender might use special category data (e.g., regular subscription to a trade union) as the basis for exclusion, or use data to identify vulnerable times for customers and target them with unaffordable credit.

**The Barriers**

One TPP stated that the ecosystem needs more time to further enhance and develop these models (for example, bank transaction categorisation is not mature) and creating robust models requires large volumes of data which will accumulate over time.

Several TPPs highlighted key challenges to using AIS data in credit decisioning today including:

- Bank transaction mutability needs to be resolved. It is imperative that data is accurate if it is to be used for fraud, underwriting and credit risk purposes – especially when credit is of a high value. A company must be convinced that the transactions are a realistic view of an account and something that can be relied upon.
- Transaction IDs are optional within the Standard (according to one submission, two CMA9 banks and one non CMA9 provide no transaction ID), and those that are provided have been shown to be erroneous in the past. It is vital that TPPs have a reliable method of deduplicating transactions themselves.
- Many other key data elements that are critical for credit decisioning are currently optional within the Standard and not commonly supplied.

- The quality of transaction information is inconsistent between banks resulting in difficulties in accurately and reliably identifying both sources of income and other lending commitments. For example, a mortgage provider may not be identifiable from existing transaction data. It was suggested that a step to resolving this would be requirements to supply:
    - Inbound "Sent from" details for bank transfers: account code, sort code and account name.
    - Outbound "Sent to" details for bank transfers: account code, sort code and account name.
    - Unique transaction code for consolidating / netting between accounts across banks.
- Significant variation in how merchants are identified in transactions making it difficult to accurately build up picture of an applicant's expenditure. Making it simpler to identify merchants would be beneficial to businesses reliant on open banking data and drive better outcomes for customers.
- Lack of meta-data around banking products. For example, credit limits and interest rates for credit cards and overdraft limits for current account. Currently only four of the CMA9, and no non-CMA9 banks make Merchant Category Codes and Merchant Names (which are optional fields within the standard) available to TPPs. This gives ASPSPs a competitive advantage over TPPs when it comes to categorising customer expenditure.
- Lack of identity data that could help with ID&V or KYC.
- Opening up access to HMRC data such as Value Added Tax (VAT) returns and Pay As You Earn (PAYE) data would be very helpful, in particular for assessing smaller/unincorporated SMEs where there are no regular management accounts.

#### *1.21.2.6. QUESTION 2.6: Error messages*

***We have asked the ecosystem sprint to consider error messages and, in particular, the additional fields needed, and the costs associated with those. From a data sharing perspective specifically, please highlight if there are any messages of particular importance.***

**Areas of Discussion**

TPPs reported that error codes are inconsistently used and lack detail to provide the TPP with sufficient information to determine the underlying cause of failure and communicate these with the customer to take the appropriate next steps. For example, one TPP provided evidence that when attempting to refresh a customer's account with the latest transaction data, error messages are received which says the account is invalid, but from that it is impossible to determine whether it is because the customer has revoked consent, the account has been closed, or perhaps the customer themself no longer has access to that account. This issue is most acute with payments, resulting in customers having to make several attempts to complete a transaction, adversely impacting customer experience, but impacts data propositions such as cloud accounting too. TPPs indicated that it was important to know if an error is transient and likely to resolve without any action, or whether the customer needs to authenticate again.

Evidence was provided showing that there was inconsistency in how error codes were provided, with the location of this data varying depending on bank, and endpoint. TPPs provided evidence that there is great difficulty in mapping and cleaning this data.

However, several banks noted that a recent review commissioned by the OBIE had found that the accuracy and consistency of error message usage was good among the CMA9 banks. It was noted that extensive evaluation of this issue had been undertaken and suggested that further analysis was unlikely to result in agreement on any further change.

Some TPPs expressed a desire to see parity with the way that error messages operate in the card networks. However, banks observed that card systems operate effectively without the reasons for errors/declines generally being shared with acquirers, processors or merchants. They noted there are also reason codes (e.g., fraud and AML related) that could not be shared, and there is a fine line between providing more detailed error messaging and providing someone with information that might prejudice an investigation, i.e., “tipping off”.

### Potential Areas of Alignment

There was a reasonable degree of support for a coordinated, ecosystem-wide approach to facilitate the standardisation of error codes. Several respondents suggested a technical working group - made up of industry subject matter experts - be convened to develop to progress this, with the Future Entity playing a central role in progressing this. No respondents provided robust data in relation to the costs associated with the introduction of additional data fields, but several TPPs indicated that improvements would reduce engineering costs, customer support costs and operational team costs. It was suggested that this might be an issue that could be evaluated by the working group. Banks were keen to have clarity at a more granular level as to when and how the provision of more data would result in better outcomes, and the specific actions that TPPs would take as a result of provision of the additional data.

### 1.21.3. Section 3: What are the longer-term changes?

#### 1.21.3.1. *QUESTION 3.1: Onward sharing and transparency*

***How should transparency and end-to-end visibility of the end recipient of data shared, including onward sharing, be improved? What are the preferred solutions and alternatives? What are the pros and cons?***

**Areas of Discussion**

**Need for greater transparency**

There were divergent views as to whether there were any issues to be solved in this space. Six responses indicated that there were limited or no problems with the way that onward sharing of data worked today. For example, one submission from an ASPSP commented that: "*The issue of data transparency in relation to customer data that is shared from ASPSPs to TPPs is already covered in the CEGs and explanatory notes available to customers when they consent for data services."* In total, responses from five TPPs and an ASPSP can be categorised in this way.

In contrast, 17 responses identified issues or areas for improvement. This included both expert advisers, most ASPSPs and a number of TPPs. This was well summarised in this response from one TPP: "*In most open banking data sharing journeys today, end-to-end visibility of the sharing taking place is simply not available or even possible."*

One TPP shared some powerful data from research they had conducted. In their research, "*74% of respondents stated they want to have control over their data (which relies on their explicit consent, rather than on implied consent) [and] 89% stated they want access to a dashboard to control their data and their consents."* ASPSPs had slightly different motivations for wanting to improve transparency, but a number supported additional transparency: "*It is important for ASPSPs to understand who the end recipient of data being shared through our APIs is [so that in ]… a data breach of an end recipient, for example, we would not have the ability to determine [who] … might be at risk."*

**Measures to improve Transparency**

There were different points of view about what measures could be taken to enhance the situation. These are broadly listed here in order of degree of support.

Eight responses considered the most effective solution to be enhancing (and potentially mandated) consent dashboards, so that they included onward sharing arrangements. "*Specifically, [consent dashboards] should be able to view a list of parties that have current access to the data".* Our understanding is that today most consent dashboards would not offer this functionality. This was typically supported by TPPs but was also proposed by a platform and one of the expert advisers.

- Seven responses proposed solutions that made any onward sharing arrangement visible at point of consent and therefore visible to the ASPSP as well as the end user. Four ASPSPs proposed this solution, as well as one of the expert advisers and two TPPs. As one of the expert advisers noted, "*There is already recognition of the challenges of unrecognised brands being involved in the value chain / data sharing."* In technical terms, a solution was proposed: "*It could be possible for TPPs to provide information relating to any onward*

*sharing as metadata within a POST request, this would enable ASPSPs (and TPPs if this information were made available via API as outlined above) to display this back to the consumer."* This potential technical solution was proposed by a TPP.

Two responses proposed that the Standard should be extended to provide more guidance and clarity of language in relation to onward sharing.

- Two responses suggested that a 'dashboard of dashboards' concept could help to bring greater transparency (this is reviewed as part of Question 3.2 below).
- One submission considered whether it would be appropriate to restrict onward sharing to parties who are regulated by the FCA (not necessarily for payment services).
- Another suggested that more work was required to consider how an end user could raise a dispute against an onward sharing party.

#### Potential Areas of Alignment

Whilst there wasn't universal support, the two following initiatives received broad support in the evidence submitted:

- Expanding the availability of consent dashboards at TPPs, ensuring that these include onward sharing arrangements and ability for end users to understand who has access to their data and stop it if they wish to.
- Enhancing the transparency of onward sharing during the initial consent journey and on access dashboards, by sharing the details of the onward sharing party with the ASPSP.

These options are not mutually exclusive and could be combined. More radical suggestions were made to limit or change rules regarding onward sharing more fundamentally, but these did not receive widespread support.

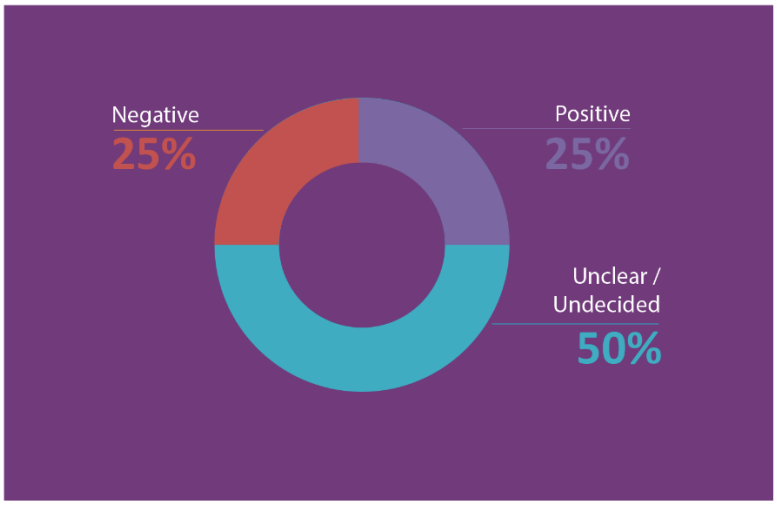
### *1.21.3.2. QUESTION 3.2: Sharing Consent Data through API*

***Could the sharing of authorisation and consent data through API be a solution to facilitate the development of secure consent management services (dashboard like features)? What are the pros and cons and costs of development? What are the challenges to implementation?***

#### Areas of Discussion

This question elicited a broad range of responses, with no clear pattern in terms of support or opposition between TPPs, ASPSPs, expert advisers and platforms. The 20 responses are summarised in figure 15 below:

***Figure 15. Attitude to sharing consent data through API***




Those positive to the idea of sharing authorisation and consent data via an API included TPPs and ASPSPs. The complexity was recognised, but one submission noted that, "*This was one of the key recommendations to come out of the recent Open Finance policy sprint held by the FCA."* This highlights an important point, that this development is closely linked to an expansion of the ecosystem, with the job of managing data connections becoming ever more complex as the number of data sources expands. A TPP noted that, "*not only will this additional data help fight fraud it will increase consumer control of their data."*

In the unclear or undecided submissions, some considered that this could become viable in the future but is not worthy of consideration today ("*maybe in the long-term, with expansion. No demand today"*). The issue of demand was also highlighted by another submission which considered that there was a very limited commercial case to develop such services and market them: "*This could be technically possible, but there is no commercial incentive for any organisation to develop this. It would be expensive to build and difficult to monetise."* One submission suggested that this could be a Government Gateway tool.

In the negative submissions, this development was seen as a distraction ("*we believe that there are higher priority issues that need to be solved first"*) or unlikely to be effective: "*We find it unlikely that most consumers would use a granular consent management platform to control the flow of their data, and we see little evidence that customers would want this. For our customer base, only around 0.5% (1 in 200) of customers make an active decision to revoke their consent."*

#### Potential Areas of Alignment

As indicated above there is limited alignment on this topic, and there seems to be limited justification to move forwards at this stage. A fair summary may be that a watching brief should be kept on this topic, particularly if and when the ecosystem expands, and new data sources come to market.

### *1.21.3.3. QUESTION 3.3: Enabling solutions for consumers in vulnerable circumstances*

***Can solutions that support consumers in vulnerable circumstances, such as bereavement, delegation of authority for accounts, etc, be developed under the current framework? What is***

***needed for such development? Do the standards need to be updated to allow for more data to be shared?***

### Areas of Discussion

Some content in this area overlaps with Question 2.3 and it is notable that a number of submissions did not provide a response to this question, potentially because they considered their response to Question 2.3 was sufficient.

Many responses focused on services for people seeking to obtain power of attorney, for example in the case of bereavement, and the role that open banking could play. For some responses, this was a niche opportunity and efforts should be focused on getting the basics right first. Other submissions noted that services already existed in this market: "*There are existing TPPs that already use open banking data to provide services related to probate and estate administration."* The Committee was therefore urged to review services already in the market or in development before considering further activity in this space.

Three responses from ASPSPs reflected the complexity in this space and suggested that the development of services may be challenging and not necessarily help consumers seeking to gain access to someone else's accounts, either for power of attorney or bereavement. One explained that: "*Bereavement and power of attorney are key use cases that support customers in vulnerable circumstances. However, challenges exist under the current framework because other data is required to verify circumstances and the identities of those involved."*

In terms of activity to support this market there were three broad areas proposed:

- **Two submissions called for a review of the economics of existing providers in this space and consideration of such services can be scaled or made more financially viable: "*What is less clear is the financial incentive for ecosystem participants to [develop services], or for the viability of any specialist providers who seek to do so*." – independent expert**
- **Four submissions noted that anyone seeking power of attorney over financial affairs would need access to a broader range of accounts, beyond payment accounts. Any service limited to current accounts, some savings and credit cards would be insufficient for most people's needs.**
- **Finally, three submissions recommended that detailed work should be done to understand the barriers and address complexity to setting up power of attorney, without compromising security. This was best summarised by a TPP: "*There are complex issues around power of attorney and access rights that need to be looked at by a standards body / regulators and the Future Entity needs to lead this discussion*."**

### Potential Areas of Alignment

This emerged from the evidence as a complex area, with some potential, but a number of significant barriers to develop and scale effective solutions to help people in vulnerable circumstances. One option for the Committee to consider would be the suggestion of a detailed review of the question of power of attorney and delegating access. This was only cited in three submissions but may have a material impact for consumers who are undergoing traumatic life events.

### 1.21.4. Section 4: Which actor(s), including the Future Entity, should play a role in operationalising the items outlined (in Sections 1-3)?

***QUESTION 4.1***

***What is the role of the Future Entity in supporting ongoing evidence collection (outlined in section 1) and the delivery of any of the changes highlighted under the short term and long-term categories (sections 2 & 3)?***

***QUESTION 4.2***

***What are the roles of industry and regulators in operationalising evidence collection and the delivery of the proposed solutions?***

***QUESTION 4.3***

***Should a premium API ecosystem develop for data? If so in what areas?***

***QUESTION 4.4***

***What is the role regulators should play? Where is regulatory intervention required and what type of intervention is required?***

#### *1.21.4.1. Areas of Discussion*

**Area of discussion 1: Data collection**

There was widespread, but not unanimous support for the Future Entity to play a role in the collection of evidence with five TPPs and two ASPSPs explicitly supporting this idea. A number of respondents, including experts, indicated the importance of gathering more data and centralisation of this process was seen as important for efficiency and consistency but the exact mechanism was not prescribed. However, one ASPSP felt that existing channels should be used for data gathering and reporting, such as the work undertaken by UK Finance on fraud rather than this activity being undertaken by the Future Entity. Two other ASPSPs felt that no decision on the Future Entity could be made until it was clear what the objectives and ambitions for open banking was. This vision and ambition would then impact the design and operation of the ecosystem and the Future Entity (or entities).

**Area of Discussion 2: Performance improvement ("levelling up")**

It was generally accepted that there was a need for the "levelling up" of the performance of ecosystem. This would lead to more consistent experiences for end users of open banking-powered services, resulting in greater confidence and growth. However, there were a broad range of views on how this levelling up could be achieved. For some, it was a matter of maturity of the ecosystem, it had already improved over time, and this would be expected to continue. However, there were also two interventions proposed to improve performance:

- **Performance monitoring and reporting**: The action of monitoring and reporting (either to a regulator or publishing) was felt to be a suitable mechanism that would lead to operational improvements.

- **Specific Performance Targets**: Another group of respondents felt that minimum regulatory targets would be needed to ensure performance. There is no reason why this could not be undertaken in parallel with performance monitoring and reporting. Expert advisers felt that regulatory backing was particularly important to ensure improved performance. This view was also shared by a number of TPPs, a number of whom indicated that this might be achieved by empowering the Future Entity.

### Area of Discussion 3: Premium APIs

Twelve TPPs, seven ASPSPs, one general trade association and one platform indicated support for the development of premium APIs. However, some of those in support did express concerns around the impact that these premium APIs would have on those APIs where access was mandated under regulation. Others suggested that now was not the time to focus effort on premium APIs:

- "[We need] *a solid commitment that standard open banking feeds continue to be available and of high-quality [when premium APIs exist]."*
- "Development of premium APIs right now would be like building a car focused on folding mirrors and a heated steering wheel while neglecting the camshaft that fires the engine."
- "Ideally open finance would be developed through the use of premium APIs, within reason. As we have learnt from the previous roll out of open banking, ASPSPs need greater incentives to invest in reliable APIs and user-friendly interfaces, though we understand that the regulator will need to be on guard against egregious pricing designed to lock out TPPs."

Others expressed doubt that the market would be able to deliver a fair and open premium API ecosystem without some form of regulatory intervention. However, two expert advisers felt that the impact of premium APIs would have such a negative impact on the market that they could not support their development:

- "I worry that a premium API ecosystem will lead to market differentiation that will benefit incumbents or those with deep financial resources supporting them. This will distort the market significantly and is unlikely to lead to optimal operations."
- "We are very concerned about the impact it will have on: the service level provided to APIs that are being used to support consumers in vulnerable circumstances [and] the commercial viability of 'for good' propositions who need a level of service offered only through a paid-for service."

### Area of Discussion 4: Timing and Prioritisation

Several of the submissions from the ASPSPs supported the need for there to be a clear vision and objectives for open banking to support progress, with two stating that no decisions about the remit of the Future Entity could be made until this vision was clear and agreed upon. The underlying theme of the responses from the TPP was one of urgency to progress at pace and that any delay to enabling further improvement and development of the ecosystem would be to the detriment of consumers and SMEs.

#### Area of Discussion 5: Regulatory intervention

A general theme from the TPP responses was an appetite for regulatory intervention to support the open banking ecosystem. There was no consensus on the exact nature of that intervention but there was a broad theme of support for a Future Entity to act with some form of regulatory backing. A platform and several banks took a different view and felt that regulatory intervention could have unintended consequences and the development of the ecosystem which should be left to market forces.

### *1.21.4.2. Emerging Areas of Agreement*

#### Future Entity responsible for Standards maintenance and development

There was acknowledgement across the respondents that standards would need to be maintained and developed where necessary, e.g., due to new regulation. Many respondents felt this would be a core purpose for any Future Entity. One ASPSP went further and felt that the Future Entity should be a standards centre of excellence able to develop standards in new areas to support the wider economy (e.g., open finance).

#### Appetite for more standardisation

There was also appetite expressed for more standardisation across the open banking ecosystem. This covered both the technical performance of the ecosystem, e.g., API performance, and the adoption of the Standard (consistent version of the Standard / usage of optional fields etc).

#### Other perspectives

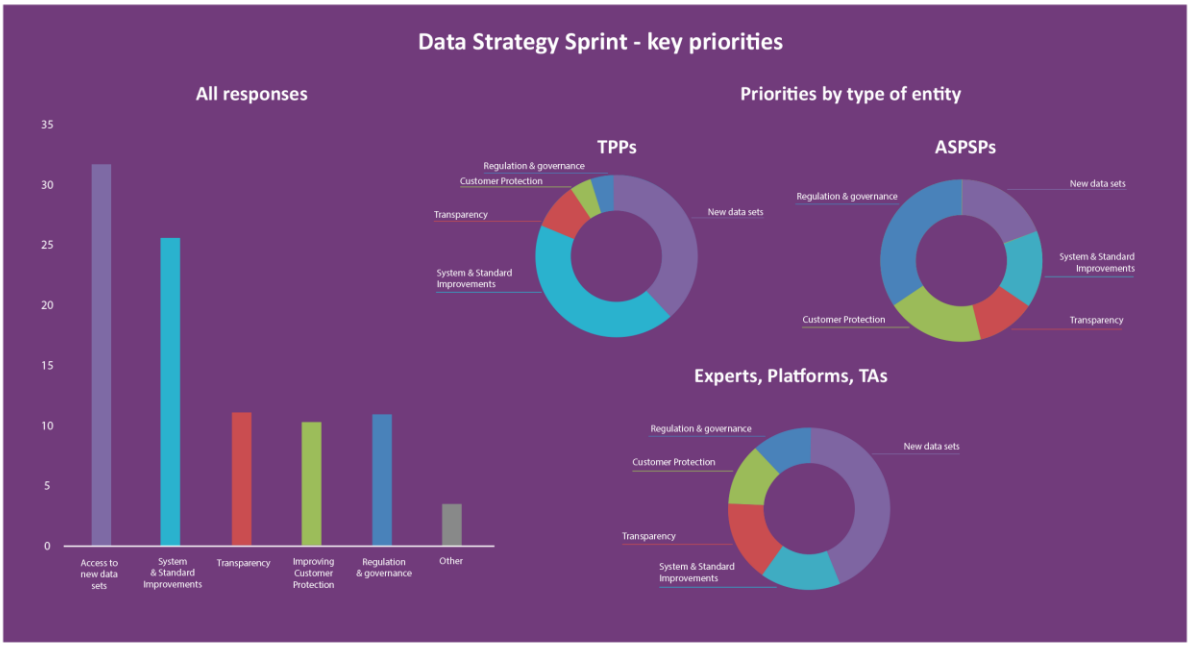
One TPP and one ASPSP expressed concern that AIS services, as a mandatory element of open banking, may be excluded from future iterations of PSD2 in Europe. They both felt that if this were to be adopted in the UK it would have detrimental effects on end users.

### 1.21.5. Question 4.5 Priorities

***What in your view are the top three short-term priorities and top three longer term priorities to be addressed in a roadmap for the future development of open banking+ payments? What would be reasonable timeframes for these to be achieved?***

Respondents gave evidence on their priorities. The different priorities have been clustered into priority themes and are summarised in figure 16 below:

***Figure 16. Key Priorities: Data***




- The ability to access new data sets was the highest priority initiative in the data sprint, but its relative priority to banks, the predominant provider of data in the short term, was lower than for other respondents.
- Ensuring that the ecosystem operates efficiently and effectively through consistent adoption of optimised standards was the other leading priority for the data sprint.
- Developing and enduring governance and regulatory framework, ensuring customers are appropriately protected and transparency to ensure customers are adequately informed were the other main priorities identified in this sprint.

## 1.22. Second Ecosystem Strategy Sprint

### 1.22.1. Section 1: What do we need more evidence on?

#### *1.22.1.1. QUESTION 1.1: Primary Research Gaps*

***Primary research with consumers and businesses, with a particular focus on vulnerable customers and small businesses, to explore key issues in relation to trust, consumer behaviour, understanding and awareness of open banking. What questions should be included? Who could deliver this and what are the best methods to follow (e.g., survey, focus groups)?***

**Areas of Discussion**

Before exploring potential research topics, questions and methodologies, it is important to highlight that a number of submissions considered that there were no gaps requiring additional insight. Two trade associations and an ASPSP challenged whether there was a need for more research and whether there were issues to explore in relation to trust or consumer behaviour. One submission made this very clear: "*We do not believe primary research on these topics is necessary*." Others suggested that greater use could be made of existing research before commissioning new research, or that TPPs should take responsibility for new research.

Many submissions expressed the need for additional insight, most strongly in the submissions from expert advisers, but also in a number of TPP responses.

Areas identified where valuable research could be undertaken included:

a) **End user understanding of open banking and terminology that could help better explain open banking.**
b) **International insights, as a way for the UK to learn from good practice and experience elsewhere.**
c) **Barriers to usage and attitudes of non-users, to understand more clearly steps that could be taken to prevent exclusion.**
d) **Improving understanding of the types and characteristics of open banking users.**
e) **An independent evaluation framework to understand the true impact of open banking on end users.**

In terms of delivery, a common theme was that research should be undertaken in partnership with industry or by other specialists in the market. Few submissions considered that a Future Entity should take forward a programme of primary research independently, preferring partnerships with TPPs or expert research organisations to generate more interesting and actionable findings.

There was limited evidence provided on research methodologies.

**Potential Areas of Alignment**

There is a strong sub-set of evidence that there is no need for new centrally commissioned primary research. However, on balance the evidence points to a need for more research, with a long list of potential topics. However, there is clear preference for research to be undertaken in partnership, with TPPs, consumer charities or with other subject matter specialists.

#### *1.22.1.2. QUESTION 1.2: Ecosystem monitoring*

***In relation to API availability and performance, including down time, response time, reasons for API failures, etc. What metrics and from whom should data in relation to conversion rates/consent success rates/ failed journeys be collected, to ensure a consistent picture across the ecosystem? How should this be operationalised, including who should take this forward, in the short-term and on an ongoing basis as open banking+ develops? Should this insight be shared across ecosystem and what is the best way to do this?***

**Area of Discussion 1: What Data Should be Collected?**

An independent expert argued that the current KPIs are inadequate, not fit for purpose and that measures such as average availability which do not tell the whole story, stating that: "*It's like having a TV and being told availability is 100% because you can always turn it on. The key statistic for a consumer is whether the channel they want to watch is consistently available, with good quality, when they want to watch it.*"

However, other respondents noted the considerable amount of work already done by the OBIE in the area of data collection, consolidation and publishing of API quality and availability metrics. These were concluded to be fit for purpose by these respondents. The primary recommendation made in such submissions was that this MI should also be collected from others in the ecosystem, beyond the CMA9 banks.

Various respondents suggested that the following metrics should be collected to give enhanced visibility of performance related issues:

- **Tickets raised and the time to resolve them in order to encourage greater internal attention and urgency to resolution of reported issues.**
- **Performance of APIs compared with banks' direct channels.**
- **API response times.**
- **API availability, including planned and unplanned down time.**
- **TPP service/app availability as this also impacts customer and the adoption of open banking.**
- **Authentication success rates, including business and technical failures.**
- **Number of steps / screens / clicks required to complete an authorisation.**
- **Conversion or completion rates as a proxy to help measure journey friction.**

Several respondents noted the importance of understanding the underlying reasons for failed payments, and the need to undertake further root cause analysis on the distribution of failed payments. One platform provider believed that synthetic testing would help prove how APIs are behaving and proposed the creation of a monitoring tool, including synthetic testing, which could be a useful feature of performance monitoring.

A trade association felt that it would be helpful to introduce mandatory real-time notifications for API availability and downtime via an ecosystem-wide dashboard.

A number of TPPs noted that the current ASPSP availability and performance reporting requirements are not fit for purpose. Statistics are sent to the FCA 'after the fact' which means that the FCA cannot be made aware of major outages in time to do anything about them. ASPSPs are also required to publish these statistics on their websites for transparency, but in some TPPs' opinions, the form they

publish them in means they are often meaningless or difficult to find. It was suggested that the FCA should review ASPSP API performance reporting.

One respondent suggested that in relation to conversion rates/consent success rates/ failed journeys, TPPs are best placed to provide this data, as they have a view across all banks of the comparative conversion rates, consent success rates and failed journeys.

Several trade associations suggested that a technical working group should be established to explore this issue in more detail.

### Area of Discussion 2: Who Should Collect Data?

Over 90% of respondents considered that collection of these expanded API performance metrics should be the responsibility of the Future Entity. However, one platform suggested that API performance is best measured by an external specialist such as API metrics, with conversion rates/consent success rates/ failed journeys provided to a central information body (similar to the Office of National Statistics) to analyse. A bank suggested that UK Finance could design and collate the MI from ecosystem participants.

A majority of TPPs recommended that the Future Entity should be given appropriate powers to consult on and introduce a standardised set of reporting standards which could be imposed on all ecosystem participants, with the necessary powers to gather the data, with the Future Entity empowered to take action to ensure the worst performers improve their performance.

An independent expert noted that: *"The Pensions Dashboards Programme (PDP) has developed a set of Reporting Standards and Auditing Standards for participants in the Pensions Dashboards Ecosystem. These apply to both Data Providers (such as individual pension schemes) and Qualifying Pensions Dashboard Services, which are the equivalent of TPPs. The Pensions Dashboards Regulations require Pensions Dashboards to enable a third-party auditor to examine and report back to the Money and Pensions Service on whether compliance obligations are being met."* This expert advocated a schedule of fines for ASPSPs, similar to those which have operated in the rail industry when Network Rail fails to deliver the required level of performance.

However, another TPP disagreed stating that API performance must be judged by the TPP: "*It is their feedback and their conversion, which counts. Not any KPIs set by a central body or even worse by API providers themselves.*"

### Area of Discussion 3: How should it be shared?

The majority of respondents agreed that insights should be shared with the ecosystem in a fair and transparent way. They suggested that appropriate industry forums and governance would need to be set up to disseminate and assess the data. One TPP stated that results should be transparent and visible, ideally with the publication of league tables showing the best and worst performers. An alternative suggestion was that banks could be obliged to publish their own results against expanded API metrics, akin to the transparency that is mandated around complaints data published by the Financial Services Ombudsman.

## 1.22.2. Section 2: What can we do in the short-term?

### *1.22.2.1. QUESTION 2.1: Adherence to Customer Experience Guidelines*

***Should TPPs and non CMA9 ASPSPs be required to adhere to the CEGs /the rest of the Open Banking Standard? What are the costs to TPPs/non CMA9 ASPSPs to implement this? What are the pros and cons and what are the mechanisms for delivery?***

#### Overview

Whilst there were some nuances in responses, a high-level analysis of responses suggests that 11 submissions agreed that there was value in the whole market adhering to the Open Banking Standard and four submissions did not.

#### Responses in support of whole of market adherence

Of the 11 submissions that supported whole of market adherence to the Standard, most saw value in the consistency, reliability and performance if all parties followed the Open Banking Standard. Expert advisers focused on the value for end users, with greater levels of trust and adoption resulting from open banking working in a predictable and uniform way across providers, "*for consumers there will be benefits in terms of simplicity and standardisation of open banking journeys"* and "*if all parties are not adhering, then the ecosystem will never gain full credibility and acceptance, and its growth/development will be stifled*". A platform came to a similar conclusion: "*Standardisation and consistency for end users helps to drive uptake, reduce journey fall out and enhance trust."*

There were variations within this group, however. One ASPSP had a view on which parts of the Open Banking Standard conformance should be required. They saw "*benefits for the ecosystem in having common security, technical, data, operational and MI standards required for all participants (TPPs as well as ASPSPs)… We do not advocate the OBIE's CEGS being mandatory for participants".*

One TPP trade association saw value in all ASPSPs conforming to the standard, but not TPPs. Another submission from the TPP community saw the value in improving the performance of the ecosystem, but considered that this should be on the basis of meeting a required conversion rate, not on compliance with specific customer journeys: "*A stronger approach would be to be clear on the outcomes desired (as data-based KPIs), and then require firms to deliver against them (either using the industry wide standards or other more advanced measures)."*

#### Responses opposed to whole of market adherence

Amongst four responses which opposed all-of-market Standard conformance, arguments focused on the strength of existing regulation ("*ASPSPs are already bound by PSD2 to apply parity between their direct customer channels and their API channel*") and the growing maturity of the market, ("*It could be (and was) helpful at the very start, but only market forces and competition will drive the necessary innovation going forward*").

Evidence was much less clear on exactly how TPPs and non-CMA9 ASPSPs would be compelled to adhere to the Open Banking Standard. Four responses suggested that some form of regulation would be required, with compliance monitored by the Future Entity. Two further responses envisaged a Future Entity with the powers "*to make mandatory requirements on a broader range of the open banking ecosystem than just the CMA9*". It was unclear how this would be achieved.

#### Potential Areas of Alignment

The evidence pointed to a broad desire to level up the ecosystem and build more consistent, high-quality journeys for end users as a driver of trust and adoption. There were many variations on how this would work in practice, what elements of the Standard it would cover, and which organisations would be in scope, but there was high level agreement on the importance and direction that should be taken. When it came to how such a programme could be implemented, evidence was much less clear, although on balance responses acknowledged that some form of regulatory intervention would be needed.

### *1.22.2.2. QUESTION 2.2: Key Aligned Messages*

***To build trust and a broader understanding of open banking, what are the key aligned messages that all participants in the ecosystem should provide throughout the user journey when consumers and business are opting for open banking services, e.g., when users are providing consent or initiating a payment? Should there be consistent messages on safety of data and connection? What are the costs and benefits?***

#### Areas of support

At a high level there was broad support for the development of aligned messages to help build trust amongst end users. Only two responses suggested that this shouldn't be a focus area, with one trade association suggesting: "*The customer experience of using open banking and the value of the propositions were more important ways to build customer confidence"* and another that, "*we have not seen evidence that there is widespread lack of understanding of or trust in open banking*."

All other responses were in favour of some level of increased alignment of messaging. This is well summarised in the following TPP response: "*Yes, messages should be aligned to ensure similar user journeys and that customers are receiving proportionate, intelligible and most of all helpful messages through the user journey".* One bank spelled out exactly what was needed: "*Costs to develop guidelines centrally are relatively small (e.g., £2-3m) and should be funded by all participants. Implementation costs will vary depending on the scope of the participant, but having messaging and terminology guidelines makes it simpler to deliver customer journeys."*

The importance of getting messaging right was underlined by one TPP response which was highly critical of the use of the term "data sharing" which connoted elements of danger or risk, although no evidence was supplied to support this opinion.

#### Additional considerations

Responses were highly nuanced. For example, a number of TPP-led responses prioritised alignment of messaging in the ASPSP domain but considered that TPP messaging should be largely left in the competitive space. This is expressed in this submission from a TPP trade association: *"Clear consent language from the TPP (in line with legal requirements) and a simple authentication journey at the bank (in line with legal requirements and CEGs) are the key to successful open banking experiences."* This tension between consistency and flexibility emerged in a number of responses.

#### Going further

Some also wanted to go further. Two submissions advocated for more clarity on messaging in regard to sharing with so-called "fourth parties" (i.e., those parties to whom data was onward shared by a regulated TPP) to be included in guidance. Two considered that a branded experience was needed, with a recognisable consumer-facing brand. Some members of a trade association saw this as

important for the longer term development of open banking payments and one independent expert considered it vital for the full development of open banking data sharing: "*To really build trust, understanding, and adoption, the key missing ingredient is a widely recognised and trusted consumer-facing brand for open banking, such as "Powered by Open Banking" or "Powered by Open Data" (along with an accompanying visual brand and/or trademark).*"

#### Potential Areas of Alignment

With two exceptions, there was broad support for more aligned messaging and language to support end user trust and adoption, and a number considered that this would be a useful activity for a Future Entity. However, there was a range of views about the extent to which this alignment should be imposed and on which actors within the ecosystem.

### *1.22.2.3. QUESTION 2.3: Dispute resolution system*

***What use cases cannot operate without a dispute resolution system? Does this system have to be centralised or can it be decentralised and located in multiple places, depending on the use case and the functions that should be supported by the system? Why or why not?***

#### Overview of the need

The majority of responses suggested that some form of dispute system was essential, particularly as open banking payments expands. Only one response suggested that there was not "*any urgency in tackling these matters via more regulation in the meantime.*" However, critically, interpretations of what a "dispute system" entailed differed significantly. In more detail:

Four responses said that no use cases could operate without a dispute system of some kind. For example, an ASPSP commented that, "*No use case can truly operate without a dispute resolution system*" and an independent expert agreed, noting that, "*all open banking use cases require the operation of a proper dispute resolution system*".

#### Payments disputes

- All other responses saw an emerging need, linked to the expansion of payments and in particular VRPs. For example, a TPP noted that a dispute system would be needed "*if we are going to move into retail e-commerce".*
- Similarly, an ASPSP commented that, "Looking forwards, we envisage that a dispute resolution mechanism will become increasingly necessary as open banking payments extend increasingly into e-commerce use cases. These will give rise to merchant disputes and other complexities that are likely to require clear processes for inter-firm data exchange and issue resolution, with appropriate data protection controls necessarily included."

#### Form of system

- There was very little alignment on what form a dispute system should take, or even if it would be correct to refer to it as a "system".
- Many responses noted that the existing OBIE Dispute Management Service had been decommissioned.
- Three responses clearly stated that a centralised dispute management system was needed. Two were expert advisers, and one was a TPP referring to a future state where there was a

need to manage disputes relating to APP fraud: "*If PISP payments are included [within the PSR's APP mandatory reimbursement regime], there will be a need for a clear, largely automated, dispute resolution mechanism to manage disagreement between PSPs on liability split.*"

Two responses preferred a decentralised disputes system, underpinned by a standardised framework, was the optimal model. This was proposed by one TPP and one ASPSP: "*A dispute resolution system should be decentralised with respect to 'point to point' processes between participants, but standards/guidance/governance and escalation would need to be centralised to be cost-effective."*

- Other submissions focused on "*a standard set of rules and procedures to be published that the whole market can follow"*, i.e., a model where firms interacted bilaterally and followed a standardised set of rules and procedures, rather than funnelling disputes through a central service. One ASPSP submission expressed this view very clearly: "*This is not inevitably a single system, it is a coherent set of operational requirements and inter-firm obligations that ensure customer issues are addressed in a timely and consistent manner, with appeals processes alongside to ensure fair treatment for all participants."*
- A number of responses were more circumspect and suggested that this was a technical area that should be reviewed and considered with care. One trade association submission called for "*the Committee to set up a technical working group - made up of industry subject matter experts, lawyers and other dispute resolution professionals - to explore the issues of dispute liability in greater depth for priority use cases.*"

#### Potential Areas of Alignment

There was clear alignment that some form of dispute system would probably be needed as open banking payments developed, particularly with expansion into e-commerce and with VRP functionality becoming more widely adopted. The nature of this system was not clear, however, and there was no common view on whether this should simply be a set of rules and standards, or a centralised function. Further work is likely to be needed to flesh out the different options and decide the best way forward.

### *1.22.2.4. QUESTION 2.4: Crisis management*

***In terms of information sharing in times of crisis (e.g., a significant breach), should the Future Entity or another actor assume the role of a facilitator and coordinate necessary information sharing and any necessary remediation across ecosystem? What detailed information should be shared?***

#### Areas of Discussion

Some TPPs noted that there are clear rules and guidance in the regulations (PSRs 2017) regarding what should happen in the case of major incident or breach participants, including incident reporting to the FCA, and reporting of data breach incidents to the Information Commissioner's Office. A risk of duplication with existing FCA oversight was highlighted if a new model were to be created. These TPPs argued that the primary responsibility in this regard for OBIE or a Future Entity, is to ensure that the OBIE Directory is treated as vital payments infrastructure with appropriate contingency measures, comparable with other such infrastructure. They noted concern that in November 2022, the OBIE Directory suffered a major incident which led to the most significant cross-industry outage of open banking since it was established.

However, many respondents considered that the Future Entity is the most obvious actor to provide a central coordinating role, and should take active steps to prepare for such potential crises, as well as to avert them. They considered that the Future Entity would be much better placed to exercise this co-ordination role than regulators due to it being likely to have the range and depth of stakeholder relationships. Respondents agreed that the Future Entity could undertake this role irrespective of whether there is a centralised directory or federated participant identity/trust model.

It was noted by an independent expert that *"while provision for this is not clearly articulated in the Australian legislation or rules, it would be reasonable to expect that the ACCC would perform this role in the absence of any equivalent to the Future Entity".*

### *1.22.2.5. QUESTION 2.5: Optional and mandatory fields*

***Under the current standards, what are the fields / guidance that is currently optional should be adopted by all ASPSPs? And what information should TPPs pass on to ASPSPs that they are not obliged to today?***

#### Area of Discussion 1: Mandating Optional Standards

The starting point for many TPPs was that, if all optional fields were made mandatory, open banking propositions would be easier to bring to market, more effective and valuable for consumers and businesses. Respondents identified the following components of the Standard that would benefit from being universally and consistently adopted.

| Component of Standard | Rationale |
|---|---|
| Transaction Value Date | Some banks do not provide this data and instead provide the "Booking Date" field. The effect of this is that some transactions are imported into cloud accounting software with an incorrect date, creating reconciliation issues. |
| Credit Card Data | In many instances, key information such as interest rates, balance transfer expiry dates and summary box information are only provided in statements. Some credit card ASPSPs make statements available to TPPs in PDF format, but this is optional. More than 60% of the consumer credit card market providers make only partial data available to TPPs. |
| Savings Offers | For savings accounts and current accounts, data fields indicating when short-term bonus rate interest rates or other offers are set to end are optional, but the information is highly relevant to consumers. |
| Error messaging | See section **Error! Reference source not found.** |

Some TPP respondents noted variability in data provided, for example, differences in the way that names were recorded or truncated by different banks, which resulted in mismatching. They recommended further standardisation to resolve this issue.

However, one TPP considered that this whole issue would be resolved by moving away from a regulatory and compliance-driven approach to a more commercial model where APIs are voluntarily provided.

Many TPPs considered that various identity attributes e.g., account opening date, account holder address, account holder date of birth etc should be made mandatory order to assist verification and as an anti-fraud measure. This was reviewed extensively in Sprint 1, see Section 1.18.3.

### Area of Discussion 2: Reciprocal obligations for TPPs

There was widespread support across both banks and TPPs for mandatory adoption of TRI data fields to improve fraud-data sharing. Banks advocated that TPPs should have reciprocal obligations in order to ensure high quality customer outcomes. Specifically, they would welcome consistent adoption of the following existing technical capabilities:

- Two-way notification of revocation by TPPs, to ensure customers get a consistent view of active services. This is particularly important for payment sweeping, VRPs and confirmation of funds checks, which all offer long lasting consent within the technical standards.
- 'On behalf of' fields within software statements, to ensure customers have clarity on the end beneficiary of an account information or payment initiation request. This is discussed in detail in Section 5.3.2.7.

Several respondents recommended that this issue would be best analysed by a technical expert group. This work should focus on intended end user outcomes and identify which data fields would be most useful to drive value for end users and allow the development of key use cases.

## *1.22.2.6. QUESTION 2.6 Error Codes*

***For response messages and error codes, the lack of granular error information was mentioned as a concern by many TPPs in Sprint 1.***

***a) TPPs and TSPs: please provide details of the priority additional data you would like to see, and when?***

***b) All participants: are there any challenges to implementation (e.g., timelines, costs)?***

### Areas of Discussion

A number of responses to this question re-emphasised the importance of standardisation in messaging and the current lack of consistency. For example, a TPP noted that, *"Error codes can be different for each ASPSP for the same error. A single standard for error codes across the ecosystem would simplify the analysis, debugging and investigation."*

The need for a valid payment status was also referenced in responses. A platform cited that significant work would need to be undertaken on the FPS platform to make this data available and the risks of doing this properly evaluated. However, some, but not all, ASPSPs are already providing up-to-date payment status information to TPPs. A large TPP suggested that they, *"Would welcome granular payment status information which updates as payments progress through an ASPSP's work queue, and also clear error coding to explain why a request is declined. This does not predicate changes in the Standards, it simply requires consistent implementation of the existing Standard across all participants."*

An area where there was some divergence of opinion was on the content of error messages. A number of TPPs felt that error messages needed to be sufficiently clear to inform TPPs or end users what actions need to be taken to resolve the issue. For example, as one TPP noted, an error message of *"OBZ08 an error has occurred"* neither informs the end user what is happening to their payment nor what they should do. Some TPPs felt that the issue was not the error codes themselves but the

use of general error codes rather than specific ones: *"[Banks use] 5xx error codes as a fig leaf to cover all sorts of unrelated scenarios including frequently failing a payment due to suspected fraud."*

However, an alternative perspective was offered by one bank who raised concerns that more detailed messaging could involve disclosing information that might prejudice an investigation, i.e., "tipping off".

#### Potential Areas of Alignment

There was a recognition that error messages were a complex area and more detailed work would be required to understand the issue and identify possible solutions. There was widespread support to undertake future work in this area.

To illustrate this, here are three representative quotes from different types of organisations:

*"We feel this question is best assessed and answered by technical expert groups. But we recognise the importance of standardising error codes to enable TPPs to understand the reasons for failures in order to communicate clearly with customers and build user confidence in open banking services. Our members have suggested that error messages around payment authorisation (PSU authentication and creation of the payment order within the ASPSP domain), and payment failure reason codes should be a priority to standardise."* – trade association

*"In principle we agree that error messages could be more consistent and detailed so that TPPs can interpret outcomes. It would be worth the Future Entity conducting an evaluation of major types of error message, plus event and status notifications, to see if they enable TPPs to fulfil end-customers' needs."* – ASPSP

*"I support the provision of granular error code information to help everyone understand why open banking consent and payment journeys are failing. The Future Entity will need to set and enforce consistent standards and collect and analyse the information."* – independent expert

### *1.22.2.7. QUESTION 2.7 Transparency*

***Enhancing transparency for end users emerged as a priority from Sprint 1. Which of the following options do you prefer to ensure that end users are clear on who they are paying or sharing data with:***

- ***i. Keep existing software statement model - no change needed***
- ***ii. Enhance existing software statement model to reduce barriers, for example by ensuring correct completion***
- ***iii. Move to identification of parties in consent flow***

***In your answer, please provide implementation considerations, including timescales and potential costs, and any required regulatory intervention.***

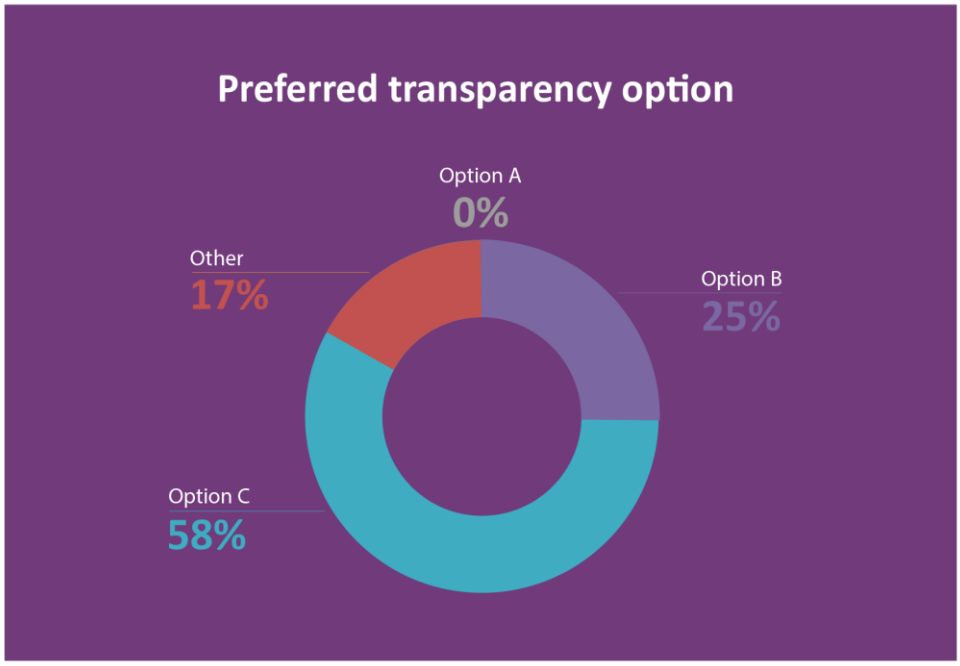
#### Areas of Discussion

The Committee set out three technical options for providing additional transparency. **Option A** is the existing model of software statements, where a TPP is required to create a separate, immutable software statement for each onward sharing party or merchant they work with. **Option B** represents an enhancement to this existing model to make it easier for TPPs to complete software statements

and register them with ASPSPs. **Option C** is a new model in which the identification is moved to the consent flow.

Of these three options, a majority of respondents favoured Option C – identification in the consent message. This model implies that when a TPP makes an access request via the API, they identify the 'on-behalf-of' field in that API request, without having to create an individual, immutable software statement for each onward shared party / fourth party. The distribution of responses is set out in figure 17 below.

***Figure 17. Preferred approach to improve transparency***




**Option C**

TPPs, platforms and expert advisers predominantly favoured Option C (identification in the consent message) as well as one ASPSP. The principal argument advanced in support of this option was that the process of creating separate software statements and then 'onboarding' them with each bank that they are connected to, acted as a barrier and that the existing software statement structure is unscalable. It was noted that the initial decision to adopt this technical design was made when access to account data was the primary use-case being considered, and in that context the solution is fit for purpose. However, the same is not true for payments where TPPs may be establishing relationships with thousands of merchants, and the process for creating and managing software statements for each merchant is neither practical nor cost-effective.

It was suggested that this is an example of where the Standard must evolve as new use cases or functionalities are adopted by the ecosystem. In these submissions, it was envisaged that the OBIE and then the Future Entity should manage this change cycle.

It was suggested by one bank that the timescales would be three months to agree Standards with all participants and c. six months to implement depending on the complexity of the requirements. This

party considered that regulatory intervention would be required to ensure all participants implement this concurrently and consistently with the agreed standards.

**Option B**

Those who favoured Option B did so largely on the basis that it is a tactical step which is likely to be achievable in a reasonable timeframe and without excessive cost of change, rather than a strategically attractive solution. Respondents felt that introducing a more substantial change would be disruptive to the ecosystem and was unlikely to be delivered before 2024.

A key issue highlighted in these responses is that, at present, it is not mandatory for TPPs to populate this information, so there is no guarantee that TPPs would do so, even if a new solution were implemented. It was noted that there has been limited use by customers of their dashboards, so the ability for this change to deliver a greater sense of end user control through increased transparency is unlikely to be achieved in the near term. It was also felt that the existing software statements are sufficient to provide end-user transparency. In these submissions, it was suggested that TPPs have an interest in accurately complete software statements to build trust and customer confidence.

**Option A**

No respondents recommended maintaining the status quo, recognising that the current situation in which the existing standards are simply not being used is unsatisfactory and change is required to address this.

**Other**

A minority of respondents recommend that more significant reform is pursued. These respondents advocated that APIs be enhanced to enable the sharing of consent information to enable a new area of competition to emerge - the provision of "dashboards of dashboards". These services would allow end users to see all the entities with whom they have granted AISP and PISP access, understand the primary value these TPPs are providing (i.e., list of use cases), and set controls to that access (e.g., revoking it, putting limits on data elements or PISP VRP parameters). This is discussed in more detail in Section 5.2.3.2 (Sharing consent data through API).

**Potential Areas of Alignment**

It was suggested by some respondents that more detailed evaluation work was required to consider and impact assess the various options. Some respondents identified was that there had been limited consideration of the ultimate outcomes-based objectives at the outset of the process, which makes it difficult to determine which, if any, of the technical solutions under consideration were most appropriate.

## 1.22.3. Section 3: What are the longer-term changes?

### *1.22.3.1. QUESTION 3.1: Delegated authentication*

***How would the implementation of delegated authentication improve consumer outcomes? What structure would need to be in place to support the delivery of this, if this were to be prioritised? What does it mean in terms of liability arrangement? What are the use cases that will benefit from delegated authentication and***

***what are the barriers and costs to implementation? Please consider international examples that could be a good reference point.***

### Areas of discussion

Some respondents saw benefits in delegated authentication. The principal benefit cited was a reduction in friction: it would "*allow merchants and PISPs who qualify and have an SCA-compliant solution to perform SCA on behalf of the issuer or accept recently performed SCA under certain conditions to reduce checkout friction*". This was a powerful benefit for some. One submission provided high-level evidence from a European market where there was, "*a sharp… increase in payment conversation for payments using delegated authentication. In contrast, SCA-compliant transactions have suffered an 11% drop in conversion rates due to purchasers needing to 'shuffle' between different apps at checkout."*

However, others remained less convinced, including a TPP trade association which "*believes that strong customer authentication of PSUs for open banking services should continue to be handled by the PSU's ASPSP. This ensures user trust and security of credentials."* Its priority was driving improvements to the redirection model rather than creating a new model. An ASPSP was of a similar view: "*ASPSPs have invested, and continue to invest, heavily to support low-friction secure authentication, and it is not clear that there could be significant benefit in Open Banking as the question seems to suggest."*

When responses turned to implementation considerations, many highlighted very significant challenges. One ASPSP summarised the work that would be required from their perspective: "*Comprehensive standards would be required and a review of the PSD2 regulatory framework with respect to a liability shift to TPPs. Contracts would need to be in place between ASPSPs and TPPs... A multilateral arrangement could support this for all participants… Standards and contract development is likely to take 12 months, followed by 12 months for implementation and testing."*

Another ASPSP had experience of implementing delegated authentication in another market and highlighted that, in their experience, it is very complex to deliver without a national ID scheme. A TPP active in this space echoed the same point, noting that, "*Successful examples of delegated authentication to third parties have relied on national ID schemes, such as in Estonia, Sweden or Finland."*

An ASPSP highlighted two additional considerations. Firstly, there could be downsides in terms of consumer outcomes: "*TPPs have commercial incentive to ensure high conversion rates of customers through their user journeys (unlike ASPSPs who are impartial). Therefore, if they are the delegate for an ASPSP there is a risk that options presented to a customer are unclear in order to encourage conversion".* Second, delegated authentication would inevitably be linked to a liability shift, which in turn may require higher capital and indemnity levels. This bank was of the view that only larger TPPs may be able to meet these higher thresholds.

### Areas of alignment

Whilst there were a number of broadly positive responses about the potential for delegated authentication to reduce friction levels (particularly in payment use cases), the level of complexity emerged as very significant. This is clearly a complex and technical initiative, particularly in a market like the UK which does not have a national ID infrastructure. A TPP summarised the position well,

saying: *"There are significant technical and regulatory challenges to this which would require considerable further investigation."*

### *1.22.3.2. QUESTION 3.2 Multilateral agreements*

***MLAs – different options were proposed by members, in particular in relation to the degree of regulatory intervention needed to enable MLAs and commercial solutions to take off. If regulatory intervention is advocated, should an approach such as the one adopted in Australia be considered where regulation provides high level principles for MLAs to be followed? What are the pros and cons of your proposed model?***

**Areas of discussion**

There was widespread support for the development of MLAs with only one platform indicating caution. The platform felt that the market was still immature and should be left to develop first. Support for MLAs came from all types of participants with a number cautioning against bilateral contracts which could distort the market. This sentiment was also reflected in the sprint discussions.

There was less detail in the evidence provided regarding the method of bringing MLAs to market. There was widespread, but not unanimous, support for some form of regulatory intervention, but the nature of that intervention was not particularly clear:

*"We believe that regulatory intervention may be needed to break the inertia and move forwards."* – trade association

*"It is unlikely that the market will be able to gain enough momentum and alignment of interests to create an open banking scheme and therefore some form of market compulsion is likely to be required."* – platform

*"MLAs and "commercial solutions" will simply not be put in place without regulatory intervention."* – independent expert

A bank and a platform both recommended that the development of MLAs should be left to the market.

A number of responses suggested that the Future Entity could play a convening role to develop MLAs and determine in what areas they would add value. One ASPSP felt the question was a little abstract, but the Future Entity could play a role when specific use cases were brought to it. Another ASPSP indicated that the development of MLAs could take a significant amount of time and they need a clear purpose to be successful.

There was no consensus on the scope of an MLA. A number of responses felt that regulators should set some parameters, in much the same way as the Euro Retail Payments Board (ERPB) set them out for the SEPA Payment Access scheme in Europe, and were set out in Australia:

*"We would recommend that parameters are set for MLAs, similar to the Australian model. However, as indicated in our previous responses, we believe regulatory intervention will be needed to unlock the next phase of open banking use cases"* – bank

*"High-level principles for MLAs seemed to have worked well in Australia."* – TPP

Other respondents envisaged multilateral frameworks as rule books overseen by the Future Entity. One respondent felt that future MLAs should be overseen by Pay.UK, but several TPPs cautioned against this on the grounds that Pay.UK would have competing priorities. An independent expert

warned against allowing big banks to dominate the development of future agreements. Some respondents felt that an MLA could form the basis of a scheme, and this would potentially be a mechanism to ensure conformant and performant solutions offered to end users.

#### *1.22.3.3. QUESTION 3.3: Combined AIS / PIS Consent*

***We have received feedback from Sprint 1 and directly that a single AIS/PIS authentication could improve customer experience. Do you agree and what are the key considerations, including costs and challenges to implementation?***

**Areas of Discussion**

Overall, seven responses indicated a level of support for a combined AIS/PIS authentication, but there were only two strongly positive responses. One of these very positive responses described this as a "*no brainer*" and the other stated that, "*We propose a new standard is developed for single authentication and consent for combined data and payment services*." The other responses in favour of this change were more guarded in their support, for example, "*We agree in principle with taking steps to improve the customer experience, including potentially the single AIS/PIS authentication, but would need to see a detailed proposal for implementation before we could make an accurate assessment of the costs and benefits of such a change."*

There was only limited analysis of how this change could enhance the customer experience with a number of responses referring to reduced friction in quite generic terms. It was notable that there was no customer research cited in support of this initiative. Some responses went further to articulate the benefits from a customer perspective. One referred to "PISP+": "*there are certain use cases (often referred to as PISP+) in which such authentication processes might be advantageous*".

One submission referred to the potential and demand for such combined propositions: "*Many businesses want to use both AIS and PIS to enable a payment and verify a user's identity or account ownership at the same time (a powerful and in-demand application of open banking). However, under current standards, the payment service user has to authenticate both the payment and data access separately in their banking app. This leads to a very burdensome and dissuasive user experience and leads to low levels of conversion."*

The implementation of this change emerged in evidence as complex, which is probably a key explanation for the guarded support indicated above.

The change would require a new standard and associated CEGs and error codes. This journey was noted as being outside PSD2 and would therefore also require new contractual structures. One ASPSP set out the scale of work required: "*The implementation cost and complexity of moving from the current approach to unified authentication is not to be underestimated. In particular, it would require an entirely new set of user journeys to be developed in online and mobile channels – this is a relatively costly change*."

One other consideration was the need to ensure that customers were clear what they were signing up to. In the views of an independent expert, it was a risk of "*a lack of clarity for end users about which precise service they were using".* The risk of inadvertent data sharing was an important consideration for two submissions, which suggested that these journeys would "*require extremely clear comms at the TPP end and would require the TPP customer experience to be considerably more prescriptive than today"* in the view of an ASPSP.

It is important to note that a number of participants did not submit evidence on this question and many responses were very high level, suggesting that this may be a technical area which has not yet received significant levels of scrutiny or consideration.

#### Potential Areas of Alignment

Overall, the evidence submitted demonstrated limited support, with the exception of two strong advocates for this change. In part, the limited support is explained by an awareness of the complexity of introducing this change. This is well summarised by the views of one ASPSP: "*We doubt that the reduction in friction is worth the expense of a significant API rebuild, and question how the customer's interests/avoidance of confusion are assured in such a journey."*

### *1.22.3.4. QUESTION 3.4: Multiple authentications*

***What changes would need to take place to enable multiple authentications for SMEs, and what use cases would this support?***

#### Areas of Discussion

There were very limited responses to this question, with many participants not providing a response.

Three ASPSPs provided responses, all of which effectively said that the Open Banking Standard already supported multi-auth flows: *"API standards already exist for the multiple authentications for SMEs and have been implemented in 2019 in compliance with PSD2."*

Two responses gave a different perspective. A TPP association suggested that the RTS had been developed with a consumer in mind and that more work may be required to adapt this for small business customers: "*The RTS authentication stipulations were designed for consumers. They should be revised for SME and business authentication. This should be done in a way where either the TPP can handle/map the company's internal authorisation procedures towards accessing their account, or simply acting on behalf of one of more company employees, where the company's procedures are already configured in their ASPSP account."*

Another TPP association suggested that cloud accounting players were better placed to manage multi-auth flows, and banks should focus on executing instructions: "*For any ASPSPs currently offering multi-auth, they should allow PSUs to disable the multi-auth on their online banking so that the relevant workflow can be handled by specialised software outside of the banking flow.*"

#### Potential Areas of Alignment

The limited number of submissions and familiarity with this aspect of open banking suggests that more work may be required with technical specialists. In effect, we were provided with three submissions from banks suggesting that multi-auth was implemented and complete, and two TPP submissions suggesting interesting ways in which open banking should be adapted for small businesses. Moving beyond this is likely to require focused work with technical experts, including providers of cloud accounting, SME payment specialist TPPs and SME experts in ASPSPs.

### 1.22.4. Section 4: Which actor(s), including the Future Entity, should play a role in operationalising the items outlined (in Sections 1-3)?

#### *1.22.4.1. QUESTION 4.1 Role of the Future Entity*

***What is the role of the Future Entity in supporting ongoing evidence collection (outlined in section 1) and the delivery of any of the changes highlighted under the short term and long-term categories (sections 2 & 3)?***

There was broad agreement that the Future Entity (or entities) should progress solutions to the priority issues around which there is consensus or those that are regulatory-driven. There was widespread agreement that data capture and evidence collection is an essential element of the entity's role. It needs to collate, aggregate and publish data from all players. Many respondents agreed that this role should extend to the collation of conformance and performance data on all participants, monitoring and 'levelling up' the entire ecosystem.

Most respondents favoured a centralised model whereby the Future Entity assumes responsibility for ensuring the constant evolution of the ecosystem, i.e.

- Delivering core infrastructure services needed across the ecosystem (immediate requirement).
- Maintaining and updating the Standards and guidelines (short term priorities).
- Driving the implementation of the strategic roadmap (longer term).

Many contributors added commissioning primary research to this list, in order to support the development of the Standards/guidelines, or inform decision-making.

However, one respondent recommended that evidence collection should be outsourced to parties for instance, the new Centre for Finance, Innovation and Technology (CFIT), with the Future Entity leading on commissioning, analysing and actioning. Some TPPs felt that it was important to establish a principle that the Future Entity only undertakes activities that the market is unable to, to keep costs down and allow the market to naturally evolve.

Most TPPs and a few ASPSPs suggested that the entity should be empowered with a regulatory mandate to implement the next phase of open finance and be the default implementation body to help implement cross-economy smart data sharing. Expert advisers agreed and considered that it was essential for the Future Entity to be given clear responsibilities and powers to set standards for the ecosystem, and regulatory authority to require the provision of data. They also recommended that it should have an explicit regulatory-set objective to act in the best interests of end users and to promote competition, with strong end user representation to support this.

However, one platform and a TPP suggested the primary role of the Future Entity should be a convenor of discussions between the various different market participants, but not a decision-making body. It was noted that the European Payments Council might be an appropriate model for the Future Entity, although not exclusively limited to payments.

#### *1.22.4.2. QUESTION 4.2: Regulatory and legislative changes*

***Where will regulatory and legislative changes be required in supporting the delivery of the proposed solutions? In what other ways can JROC facilitate progress, e.g., roundtable, industry sprints?***

This question focused on priorities for the Committee in supporting the effective development of open banking payments and data sharing. As it was worded as an open question, there were a wide range of proposals submitted in evidence which are summarised below.

### Regulatory and legislative framework

The most commonly cited area of proposed focus was to ensure that open banking has the right regulatory and legislative framework to move forward effectively. Many respondents saw this as a critical role for the Committee. For example: "*There now needs to be action from the Government to lay the legislative grounds for a Future Entity that has the ability to direct the open banking ecosystem to ensure good outcomes for consumers and businesses through the further development of innovative open banking services."*

Another response called for, "*The expansion to open finance (and beyond to open/smart data) to be put on a regulatory footing, by including it in the Data Protection and Digital Information Bill expected to come to Parliament in Q4 2022 or Q1 2023. This would create a legislative, rather than competition, mandate for data holders in the UK to open up their data sets via API."*

### Commercial structures

The second most commonly cited area of Committee activity was in addressing the commercial structures underpinning open banking. This request came from both ASPSPs and TPPs, with six responses looking for the Committee to *"define the parameters of the economic model(s)*". This work was closely linked in many responses to a role in supporting the emergence of MLAs to develop the market.

### Vision for the market

The third area was to set a vision for the market, for example one response called for the Committee to *"develop a coherent overarching policy framework and clear expectations for the future of open banking payments".* This was also seen in relation to open finance, with many responses looking for the Committee to drive the expansion of the data sharing ecosystem. There was also an expectation that the Committee would continue to consult and engage with the market after the completion of the current work of the SWG, particularly around the composition of any new roadmap.

### Future Entity mandate

Finally, a number of responses called for the Committee to ensure that the Future Entity was successfully established and had an appropriate mandate to develop the market. For example, one response called for the Future Entity to be given "*powers to set binding Standards*".

As a counterpoint to these submissions and calls for a proactive approach from the Committee, one response called for less regulation and less intervention: "*Any regulation should be minimal and outcome driven. Currently, there is too much of it, and it is too technical, and both are stifling innovation and competition... This should be replaced by creating the right incentives… for the market to self-regulate*."

### Potential areas of alignment

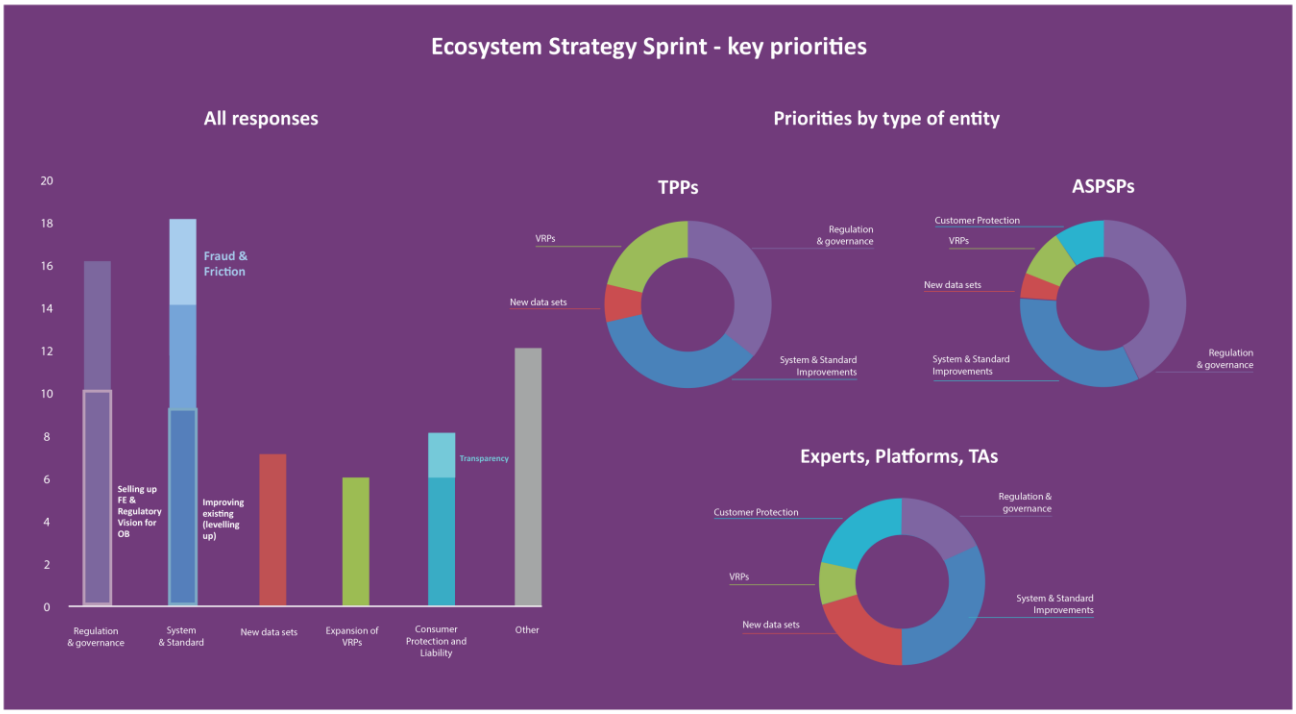
Whilst there were a wide range of responses and proposed areas of focus, overall, there was broad alignment about wanting the Committee to take a proactive stance on issues such as evolving regulation, addressing commercial structures, encouraging the emergence of multilateral frameworks and setting the vision for the next stages of open banking payments and data sharing.

### 1.22.4.3. QUESTION 4.3: Priorities

***What in your view are the top three short-term priorities and top three longer-term priorities to be addressed in a roadmap for the future development of open banking+?***

Respondents gave evidence on their priorities. The different priorities have been clustered into priority themes and are summarised in figure 18 below:

***Figure 18. Key Priorities: Ecosystem***




- Improving the operation of the ecosystem through consistent adoption of an optimised Standard was identified as the highest priority in responses to the Ecosystem Sprint. The objective to level up performance to the higher performing firms and having an appropriate approach to target friction at higher risk transactions were key elements of this priority theme.
- Ensuring a consistent and enduring regulatory and governance framework was also a key priority in the Ecosystem Sprint. Setting up the Future Entity with appropriate governance and regulatory scrutiny was the main component of this theme.
- Key priorities from the payments and data sprints such as customer protection, accessing new data sets and expanding access to VRPs beyond sweeping also emerged as key priorities in the Ecosystem Sprint.

### 1.22.4.4. QUESTION 4.4: Central Standards Setting

***Should the Future Entity assume the role of a central standard setting body to develop, maintain and monitor future Open Banking Standards or do more/less? If not the Future Entity, whom? How is competition best ensured?***

### Broad support

There was very strong support across all types of respondents that the Future Entity should assume the role of a central standard setting body to develop and maintain future Open Banking Standards. The following points were made in support of this:

- The Future Entity (or entities) should co-ordinate the implementation of future standards and provide tools to assure participant conformance with those standards. (It was noted that the existence and role of the OBIE had been critical to the progress of UK open banking to date, with some respondents keen to ensure that the considerable investment made in the OBIE was leveraged so far as possible).
- The OBIE (and, it is expected, its successor body) is the only organisation which has the technical experience to take forward open finance and open data initiatives in the UK, and as a result the Future Entity also be given a role in standards setting for these initiatives. In their view, a multiplicity of standards setting bodies would be inefficient and unworkable as financial and non-financial data become increasingly commingled in future use cases.
- Broadening the scope of the central standards body into other sectors may help resolve issues around funding, and reduce reliance on the CMA9.

### Minority dissenting views

There were some dissenting voices. One submission suggested that these functions could be transferred to Pay.UK. It argued that it would be more cost-effective for Pay.UK to become the central standards body, using existing capability, rather than setting up a new entity. One submission suggested that the UK required a "*European Payments Council-style Future Entity, which is not limited to payments, but flexible to address and encompass all the upcoming "payments-related" matters as well."* One submission felt that clarity was needed on the type and scope of standards development.

### Additional considerations

Governance was a key point raised, as a qualifier to the support set out above. One submission emphasised that a central standards setting body should not preclude the development of other schemes, such as Europe SPAA or TISA UK. An independent expert supported the Future Entity assuming this role on the proviso that it has clear objectives to act in the best interests of end users and promote competition.

Although this was not raised in the question, a number of submissions said that the Future Entity should become a standards setting centre of excellence across all data sharing initiatives. This was most clearly expressed by an ASPSP, which stated that: "*We consider there to be a compelling case for a single centrally governed and funded standards body in the future state. Ideally, standards should be designed to be interoperable across the economy… For example, in the future state a single certificate design should identify the firm as a party across multiple open domains (open banking, open insurance, open retail, open energy). Similarly, common security standards and customer authentication processes will enable composite products to be created."*

#### International comparison

Bringing in a perspective from Australia, an independent expert noted that, "*The only new body established for the purpose of the Australian CDR was the Data Standards Body, now part of the Australian Treasury, which assists the independent Data Standards Chair in making the standards. The CDR Rules require the Data Standards Chair to establish an advisory committee which is required to have a consumer and a privacy representative, and provides the ACCC, the Australian Office of the Information Commissioner and the Department of Treasury with the right to join as observers. In addition, the CDR Rules require the Data Standards Chair to engage in public consultation before making or amending a data standard. The Australian Standards are required to be published on the internet and available for free.*"

### *1.22.4.5. QUESTION 4.5 Funding*

***How should a central standards body be funded, for example tiered membership, regulatory levy, annual fees or a pay-for-use model? Should fees be based on market size, API numbers, customer base or other metrics?***

#### Areas of Discussion

A common theme running through the responses was that any future funding model needed to be fair and equitable. These sentiments were echoed by all the stakeholder groups, but the model of how this might be achieved differed, for example:

- *"[We] need a detailed debate to agree a fair and equitable funding model."* – independent expert

*"The funding approach should also be fair and proportionate and is likely to require a tiered model whereby fees are determined by the type of participation (and the services accessed beyond standards use)."* – trade association

"The central standards body should be funded by data holders (ASPSPs) and third party providers who connect directly to the APIs provided by the ASPSPs." – TPP

- *"The entity could be established with the same funding model as the FCA and funded by the entities it regulates."* – TPP
- "Fairest way to fund a central body is on usage." – platform
- "A tiered levy on data providers could be explored… Strongly discourage fees linked to overall usage of open banking (e.g., volume of API calls) as this disincentivises data providers from supporting improvements to performance." – bank

"Some market participants advocate a funding model in which all PSPs would fund the Future Entity via an FCA levy (or similar mechanism) … [we] consider that ultimately this model may frustrate the market's ability and freedom to innovate." – trade association

- "An effective funding model would be flat membership fees for all Standards users, entitling them to certification tools that evidence the Standard has been implemented correctly (this is how OIDF operates, for example)." – ASPSP

Another theme that emerged was that the funding model could differ based on the services used or consumed, so any decision on funding would be impacted by the decisions on the scope and functions of the Future Entity (or entities). A note of caution was raised by an independent expert to ensure that the governance model for the Future Entity was designed so that the largest funders did

not have undue influence over the development of the ecosystem. This concern was also raised in other sprints by TPPs.

### *1.22.4.6. QUESTION 4.6 Trust Services*

***We received several responses regarding the way in which trust services (currently the OBIE Directory, including provision of certificates and NCA/FCA permissions checking). Which model of delivery do you prefer:***

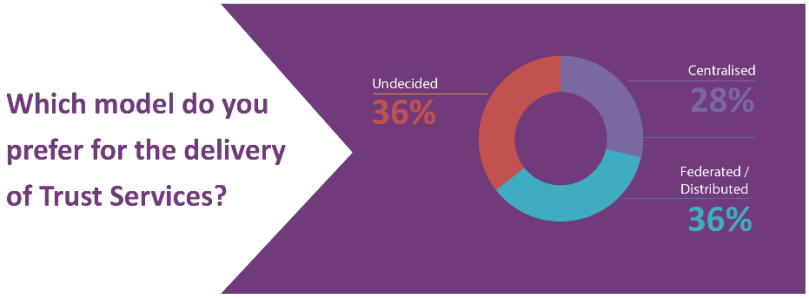
***ii. a single centralised model***
***iii. a federated model, whereby certificates can be provided by approved actors, or***
***a) another option (please explain).***

***Please explain your reasoning e.g., evidence from other jurisdictions.***

#### Areas of Discussion

There was a range of responses to this question as demonstrated in the graph below:

***Figure 19: Trust Services Delivery Mechanism***




**Federated/distributed**

Five respondents indicated that they felt a federated model was the preferred model for the future provision of trust services. This is the model adopted in Europe and provides a way to build resilience into the system:

"*Our preference is for a federated model, whereby certificates can be provided by approved actors (similar to the eIDAS model used for PSD2 in Europe)*." – bank
*"Federated model ensures risk and liability is distributed across the ecosystem and there is appropriate capital and insurance underpinning liability."* – bank
*"The Future Entity should only step into issues where industry can't provide a solution."* – platform.

**Centralised**

Four respondents felt that a centralised model would be most appropriate as it should be lower cost and would minimise risks caused by moving to another model too quickly:

"*Centralised model as federated model likely to cost more… can get value for money by conducting competitive tender for provision of the services."* – independent expert

"*Concern is that any change in supplier does not disrupt existing services or create additional burdens for TPPs (such as further enrolment, certificate issuance etc, which can all be time consuming and costly)… [the Directory] is a piece of vital infrastructure for the open banking ecosystem (as the major incident on 18 November proved). Regulators must ensure a robust resolution process for such incidents to minimise disruption to consumers and businesses using open banking."* – TPP

**Undecided / further work required**

Five respondents indicated that both models had pros and cons or felt that further work was required in order to have an evidence-based opinion:

"*[We] support a full evaluation of the most effective and efficient model for provision of directory services... should be driven by cost efficiency as well as ensuring the capability is effective and scalable."* – bank
"*Depends on JROC strategy if core infrastructure is opened up to competition means move away from centralised model.*" – trade association

### *1.22.4.7. QUESTION 4.7 Support Services*

***To deliver the vision of open banking+, what other functions should a Future Entity carry out (if any), apart from concerning standards setting and trust services? (e.g., development of multilateral frameworks, monitoring, participant support, ecosystem development and promotion). How should these be funded?***

**Areas of Discussion 1: Additional services**

Respondents identified a range of services, apart from standards setting and trust services, that they considered would be appropriate for the Future Entity to provide. These are set out in the table below with an indication of the level of support for each of these from respondents, based on the percentage of all respondents identifying the need for a particular service.

| Function | Future Entity role | Share identifying need for service |
|---|---|---|
| **Participant conformance and performance** | • Monitoring (either directly or supplying regulators with data)<br>• Provide conformance tools<br>• Assure participant conformance<br>• Maintain MI specifications<br>• Collect/collate conformance & performance data on all participants | 38% |
| **Development of multilateral frameworks** | • Development, implementation, maintenance and governance of multilateral arrangements | 54% |
| **Develop an A2ART scheme** | • Development of common rules, pricing, trust mark | 8% |

| | | |
|---|---|---|
| **Participant support** | • Maintain help desk<br>• Maintain participant forums<br>• Share insight from ecosystem and participants | 31% |
| **Ecosystem development and promotion *** | • Promoting awareness of the ecosystem<br>• Building consumer trust<br>• Educating users about the use of open banking | 31% |
| **Dispute management and resolution processes** | • Develop mechanisms to assist participants resolve complaints and disputes | 15% |
| **Onboarding** | • Provide a test environment and support for new participants | 8% |
| **Crisis Management Co-ordination** | • Role of facilitator and coordinator following a crisis | 8% |
| **Independent evaluation / Customer Evaluation Framework** | • Gathering and publishing the research and MI necessary to evaluate open banking | 8% |
| **Ecosystem governance and collaboration** | • Ecosystem governance to set/deliver strategy<br>• Future Entity governance to manage organisation<br>• Participant forums to provide input on issues and priorities | 31% |

**No respondents stated support for the Future Entity having a role in 'marketing' open banking.*

### Area of Discussion 2: Funding for Support Services

Respondents put forward similar comments similar to those expressed in response to Q4.5 (See Section **Error! Reference source not found.**) and indicated that participants should fund these services. Some respondents favoured a pay for usage model, while others suggested a tiered approach to ensure alignment with ability to pay and not acting as a disincentive to competition. It was suggested that the pricing model applied might differ depending on the service being provided.

# APPENDIX 1: Glossary

| | |
|---|---|
| AIS | Account Information Service, the provision of account information service carries out by an Account Information Service Provider (AIPSP), which is authorised and regulated by the FCA. |
| A2A | Account-to-account payments |
| A2ART | Account-to-account retail transactions |
| API | Application Programming Interface, a way for two applications to communicate with each other. |
| APP | Authorised Push Payment, usually used to refer to APP scams. |
| ASPSP | Account Servicing Payment Service Provider (ASPSP) is any financial institution that offers a payment account with online access. This includes banks and building societies. |
| BCA | Business Current Account |
| BEIS | Department for Business, Energy & Industrial Strategy |
| CMA Order | The retail banking Market Investigation Order 2017. |
| CMA9 | The nine largest banks and building societies in Great Britain and Northern Ireland, based on the volume of personal and business current accounts. AIB Group (UK) plc trading as First Trust Bank in Northern Ireland, Bank of Ireland (UK) plc, Barclays Bank plc, HSBC Group, Lloyds Banking Group plc, Nationwide Building Society, Northern Bank Limited, trading as Danske Bank, The Royal Bank of Scotland Group plc, Santander UK plc (in Great Britain and Northern Ireland). |
| Commercial VRP | Often referred to as “non-sweeping VRP”, a Variable Recurring Payment that is outside of the CMA Order requirement on the CMA9 to provide free access to the VRP API. |
| CoP | Confirmation of Payee – an account name checking service |
| Conversion rate | Also known as “Consent Success Rate”, the proportion of customer journeys that are successfully completed. |
| CRM Code | The Contingent Reimbursement Model Code, designed to reduce the occurrence and impact of APP scams. |
| EPC | European Payments Council |
| ESG | Environmental, Social and Governance |
| JROC | Joint Regulatory Oversight Committee, comprising the FCA, PSR, CMA and HMT, and responsible for the future of open banking in the UK |
| KYC | Know Your Customer, i.e., the processes carried out by firms to ensure an organisation is appropriately identified. |

| | |
|---|---|
| NPA | New Payments Architecture |
| OBIE | The Open Banking Implementation Entity |
| Pay.UK | The UK's account-to-account payments operator. |
| PCA | Personal Current Account |
| PDP | Pensions Dashboards Programme |
| PIS | Payment Initiation Service, the initiation of a payment from a customer's account carried out by a Payment Initiation Service Provider (PISP), which is authorised and regulated by the FCA. |
| Platform | For the purposes of this report, a payments scheme or operator, standards body or large digital technology provider. |
| PSD2 | The Second Payment Services Directive |
| PSRs 2017 | (PSR) The Payment Services Regulations 2017, the UK's implementation of PSD2, as amended or updated from time to time and including the associated Regulatory Technical Standards as developed by the EBA. |
| SEPA | Single Euro Payments Area. Often used to refer to payment schemes for the euro area, such as SEPA Credit Transfers. |
| RTS | Regulatory Technical Standard |
| RFID | Radio-frequency identification |
| Sweeping | Sweeping is a generic term for the movement of funds between a customer's own accounts, a "me to me" transaction. For the purpose of the Order, the CMA has published further clarification[9]. |
| SWG | Strategic Working Group, a non-decision making consultative forum on the future of open banking. |
| TISA | The Investing and Saving Alliance, a financial services trade body |
| TPP | Third Party Providers are organisations or natural persons that use APIs developed to Standards to access customer's accounts, in order to provide account information services and/or to initiate payments. Third Party Providers are either/both Payment Initiation Service Providers (PISPs) and/or Account Information Service Providers (AISPs). |
| TRIs | Transaction Risk Indicators, designed to help Payment Services Providers understand more about the fraud risk of a particular transaction. |
| Trust Services | The range of services provided to ensure a high level of trust is maintained in the digital ecosystem, this could include checking of identity, issuing and checking of digital certificates, checking validity or permissions to undertake specific activities |

[9] https://assets.publishing.service.gov.uk/media/622ef71fd3bf7f5a86be8fa4/Sweeping_clarification_letter_to_be_sent_14_March_2022__.pdf

| | |
|---|---|
| VRP | Variable Recurring Payment. A VRP is a mechanism to make one or may payments over a period of time using open banking. The Payments need to fall within the VRP Consent Parameters which must be authorised by the Payment Service User (“PSU”) via Strong Customer Authentication (“SCA”) at their ASPSP. |

# APPENDIX 2: Members of Expert Panels and Strategic Working Group

## Open Banking Strategic Working Group Members

- **Ghela Boskovich, Regional Director, FDATA**
- **Matt Cox, Lead Member, Project Open Banking, The Payments Association**
- **Tony Craddock, Director General, The Payments Association**
- **Charlotte Crosswell, Chair and Trustee, OBIE**
- **Charles Damen, Chair of Open Banking Working Group, UK Finance**
- **Matt Davies, Senior Policy Advisor, ODI**
- **Nilixa Devlukia, Chair, Open Finance Association**
- **Scott Farrell, Payments Expert, Independent**
- **Kate Frankish, Chief Business Development Officer, Pay.UK**
- **Adam Gagen, SWG Lead, Innovate Finance Policy Committee, Innovate Finance**
- **Dan Globerson, Chair of Open Finance Steering Group, UK Finance**
- **Chris Henderson, Chair of Open Banking Payments Working Group, UK Finance**
- **Janine Hirt, Chief Executive Officer, Innovate Finance**
- **Philip King, SME Expert, Independent**
- **Dominic Lindley, Consumer Expert, Independent**
- **Jana Mackintosh, Managing Director, Payments and Innovation, UK Finance**
- **Ralf Ohlhausen, Chair, ETPPA**
- **Thaer Sabri, Chief Executive, The Electronic Money Association**
- **Dan Wilson, Member of Open Banking Working Group, The Electronic Money Association**

**Representatives from the FCA and PSR, CMA and HMT may attend SWG meetings as observers.*

## Open Banking Payments Expert Panel Members

- **Louis Adamou, Technology Director, Loaf**
- **David Bailey, COO Payments, Santander**
- **Stuart Bailey, Head of Payments Industry and Regulation, Lloyds Banking Group**
- **Stuart Barclay, VP Strategy, Volt**
- **Jessica Bilcock, Public Policy and Vulnerability Manager, Monzo**
- **Tim Birts, Senior Product Owner, Nationwide**
- **Mike Chambers, Chair, Answer Pay**
- **Adnan Chowdhury, UK Policy & Government Relations Lead, Wise**
- **Todd Clyde, CEO, Token**
- **Duncan Cockburn, CEO, OneBanx**
- **Holly Coventry, VP International Open Banking Payments, AMEX**
- **Florence Diss, Head of EMEA Commerce Partnerships, Google**
- **Mick Ebsworth, Director Information Security, Co-op**
- **Mark Falcon, Payments Expert, Independent**
- **Paul Foster, Director - Global Payment Partnerships, GoCardless**
- **Tony Herbert, Senior Policy Advisor, Which?**
- **Charlie Humphreys, Director Apple Pay and Wallet Services Northern Europe, Apple**
- **David Jones, Director Payment Innovation, Strategy and Planning, Barclays**
- **Mark Jones / Nigel Partington, Overlays Product Manager, Pay.UK**
- **Matthew Lane, Head of Europe, Open Banking & Real-Time Payments, Visa**
- **Kris Lindquist, Principal Product Manager - Bank Payments, Amazon**
- **Colm Lyon, CEO & Founder, Fire**
- **Andrew McClelland, Insight Expert, IMRG, UK E-Commerce Association**
- **George Miltiadous, Head of Open Banking Delivery UK, HSBC**
- **Dan Morgan, European Policy Lead, Plaid**
- **Ciaran O'Malley, VP Financial Services & E-commerce, Trustly**
- **Maria Palmieri, Director of Public Policy, Yapily**
- **Hannah Regan, Head of Finance Policy, British Retail Consortium**
- **Lynsey Rodger, Policy Analysis Manager, NatWest**
- **Ralph Rogge, CEO and Co-Founder, Crezco**
- **Conor Tiernan, Commercial Manager - Open Banking & Bank Payments, Klarna**
- **Craig Tillotson, CEO, Ordo**
- **Jim Wadsworth, SVP Open Banking, MasterCard**
- **Jack Wilson, Head of Public Policy, Truelayer**

**Representatives from the FCA, PSR, CMA and HMT may attend Payment Expert Panel meetings as observers.*

## Open Banking Data Expert Panel Members

1. **Gary Aydon, Project Delivery Manager - Open Banking, Santander**
2. **Louise Beaumont, SVP Global Open Banking & Open Finance Industry & Policy, Mastercard**
3. **Will Bolton, Open Banking Lead, Account Technologies**
4. **Rob Burlison, Director of International Corporate Affairs, Intuit**
5. **Albert Cabré Juan, Open Banking Lead, Monzo**
6. **Gerald Chappell, CEO and Co-Founder, Fintern**
7. **Kat Cloud, UK Public Policy Lead, Plaid**
8. **Conor D'Arcy, Head of Research and Policy, Money & Mental Health Policy Institute**
9. **Pradeep Dhananjaya, Tech Banking Lead, Amazon**
10. **Michael Forrest, Enterprise Architect 2013 Digital Identity and Open Banking, Barclays**
11. **Manish Garg, CEO, Banksly**
12. **Gabrielle Gleeson, Strategic Operations Director, TotallyMoney**
13. **Michael Green, GM Partnerships, UK and EMEA, Xero**
14. **Brian Hanrahan, CEO, Nuapay**
15. **Rob Haslingden, Head of Propositions & Product Marketing, Experian**
16. **Chris Jones, Chief Product Owner – Industry API, Nationwide**
17. **Glen Keller, Chief Product Officer, CRIF Realtime**
18. **Adam Khalifa, Head of EMEA Financial Services, Google**
19. **Paul Lloyd, Co-founder and CMO, Snoop**
20. **Andrew Millar, Global Head of Strategy Planning and Policy OBSS, HSBC**
21. **Paul Mortby, Head of EMEA Policy, Block**
22. **Lisa Pearlman, Director Global Policy, Apple Inc**
23. **Adam Prince, VP Product Management, Sage**
24. **Kiran Rajulupati, Product Owner, Yapily**
25. **Dan Scholey, Chief Commercial Officer, Moneyhub**
26. **Archi Shrimpton, Senior Manager Open Banking, Lloyds Banking Group**
27. **Andy Sleigh, CEO, Clearscore**
28. **Bee Thakur, UK Public Policy Lead, Truelayer**
29. **Polly Tolley, Director of Impact, Citizens Advice Scotland**
30. **Jonathan Turner, Technology Strategy and Innovation Lead, Fair4All Finance**
31. **Jan van Vonno, Head of Industry Strategy, Tink**
32. **Daniel Weaver, Chief Product Officer, Smarter Contracts**
33. **Harry Weber-Brown, CEO, TISA Digital**
34. **Edgar Whitley, Associate Professor, LSE**
35. **Stephen Wright, Head of Regulation and Standards, NatWest**

**Representatives from the FCA, PSR, CMA and HMT may attend Data Expert Panel meetings as observers.*

www.openbanking.org.uk/swg