STRATEGIC WORKING GROUP – ECOSYSTEM STRATEGY SPRINT

Submission from The Payments Association

The Financial Conduct Authority (FCA) and the Payments System Regulator (PSR) as co-chairs of the Joint Regulatory Oversight Committee (Committee) have convened a Strategic Working Group (SWG) to help shape the future of Open Banking. The Payments Association has two seats on the SWG.

Members of the SWG are expected to contribute to the Open Banking Ecosystem Strategy Sprint, which will be focusing on ecosystem-wide questions as determined by the Committee.

In September 2022, the Payments Association's Project Open Banking surveyed members to collate views and input from industry and broader stakeholders to define the strategic roadmap for further development of the Open Banking ecosystem. This included 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.

Input and survey responses came from a broad range of the Payments Association's membership of 180 companies from across the payments value chain, with stakeholders' views received 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.

These responses have been collated, aggregated and anonymised below to set the agenda for the Strategic Sprint Discussion meeting.

QUESTION 1:

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?

Current standards for Open Banking are selectively applied. Companies in the CMA9 are tightly regulated and are required to submit detailed and costly MI submissions monthly by the OBIE standards, but no such controls exist for TPPs. Additionally, all of the costs of regulation and monitoring are solely borne by the CMA9. This has effectively created a two-tier approach to regulation and has resulted in several inconsistencies. Similarly, the current payments liability model is almost exclusively ASPSP-based.

In general, in an ecosystem reliant on reciprocal parties, having standards and guides for TPPs and non-CMA9 that aren't enforceable limits their effectiveness, and can lead to inconsistent consumer experiences and outcomes. Confirmation of Payee is a service where all parties are bound by the same rules and guides to ensure a consistent consumer outcome and ubiquity of adoption. Likewise, all parties in the card schemes are bound by enforceable standards, as expressed in the scheme rules.

There is a limit to the amount of guidance and standards that can continue to be supported for Open Banking under the current model, where the ecosystem is funded disproportionately by the CMA9,

despite the ecosystem's ongoing expansion beyond the scope of the Order. While OBIE has historically had an important role in setting guidance and standards for Open Banking, the future of the Open Banking ecosystem is much wider than the scope of the Order, and it would therefore would not be within its mandate for JROC to provide OBIE with an ongoing role exceeding the Order.

It is important for JROC to create an equitable funding model that does not rely on certain market participants cross-subsidising the industry. The SWG should therefore recommend a suitable alternative governance structure for the future entity that sets Open Banking on a legally sound and commercially sustainable path.

With an equitable funding model in place, there are areas where gaps could be addressed with further Open Banking guidance and standards. For example, it would be helpful for centralised standards to be implemented to create a robust dispute and liability model, and also for fraud data sharing.

Gaps in standards and guidance

There are several gaps in guidance and standards relating to payments that prevent efficient and safe customer journeys using Open Banking, and that limit adoption for wider use cases. While they are safe and efficient for the current Order use cases, they cannot be scaled for the adoption of other use cases such as ecommerce. For example:

- The existing model of liabilities and disputes for Open Banking payments, and the lack of customer protections, does not meet the quality available on alternative payment mechanisms such as cards and direct debits. Significant effort and investment are required to develop a comparable set of standards to underpin the development of these features for Open Banking
- There are currently restrictions on ASPSPs that prevent additional language, warnings or controls in Open Banking payment journeys that would specifically address consumer harms such as fraud. By comparison, in direct internet/mobile banking channels, customers are shown a range of tailored messaging targeted at reducing APP fraud. ASPSPs are prevented from doing the same in Open Banking payment journeys as part of the Open Banking Standard, even though this addition of positive friction could improve customer outcomes and prevent fraud. Some of our members have provided evidence of mitigation of fraud from card and direct payment channels to Open Banking Payments, too

In relation to payment journeys and improving the customer experience, many participants highlighted that increased data granularity would be beneficial. Many retailers and other merchants have heavily invested in fraud prevention using mitigation mechanisms and transaction risk analysis. They have the ability to assess their customer risk profile as well as the transaction risk and apply the right authentication mechanism and customer experience to the shopping journey.

One approach to improving the customer experience could be to provide or make available to the PISP the current balance of the payment account prior to and/or after payment initiation. The provision of balance to help inform the customer when they're making a payment, or where the customer needs to know how much money they have, could make for improved payment experiences. Equally if a customer has multiple payment accounts with the same institution, the balance may be a key data point in helping them select from which account they'd like to transact.

PISPs need to know confirmation of payment execution, including additional status once the payments are executed (i.e., post-initiation submission) for processing on the agreed execution date

by the ASPSP. The PISP needs to determine with sufficient certainty that the payment will be complete and subsequently can provide some certainty to the user. The earlier the merchant knows a payment is rejected, the quicker it can offer alternative payment solutions to a customer. This avoids abandoned carts and loss of revenue. Customers may incur penalty fees and excess interest if they don't know their payment has failed. This level of certainly is provided for Card based payments but not for bank to bank payments, which reflects the fundamentally different architecture that underpins them and the purpose for which (Faster Payments) was designed to support PISPs' direct channel money movements.

One approach could be a mixed AIS/PIS journey in one communication session, implying three scenarios:

a) One SCA to allow the AISP to access AIS-regulated information and one SCA to allow the PISP to initiate a payment;
b) One SCA to allow the AISP to access AIS-regulated information, and no SCA to initiate a payment in case of SCA exemption for the payment transaction;
c) One SCA to allow the PISP to initiate a payment, and immediately thereafter in the same session to allow the AISP to access AIS-regulated information.

Variable recurring payments

It was also highlighted that non-sweeping variable recurring payments could be transformational for domestic payment services in the UK, providing a much better user experience and self-service compared to direct debit and cards. Standards would need to be adopted to allow much more granular data e.g., location, for use with these payment types.

Variable recurring payments need to more closely mirror cards on file in order to open up more use cases and to improve customer experiences. Currently, variable recurring payment require continuous consents from the customer. What Open Banking is trying to do with mandates is to give more control to the payer, but this limits implementation and the ability to work as well as card payments do.

For variable recurring payments, an option could be for the payer to effectively give a mandate to the payee that they can have their account details on file and bill on a recurring basis, as an example for renewals on insurance policies, as can be done with cards.

Consents

Additional guidance to PISPs on the maximum allowable limits to be entered in a consent are required to help limit the impact of a consumer falling victim to an APP scam. During controlled customer scaling, an ASPSP observed that a consent could be created with a daily limit of £10 billion. There does not seem to be a justifiable reason for such high limits, particularly considering the use case of sweeping; movements of relatively small funds to offset unsecured debit or bolster savings on a regular, reoccurring basis. The increased risk of Fraud in this channel should also be a consideration particularly ahead of addressing functional, liability and operational gaps in such payments relative to Cards.

It highlights a gap in guidance on the level of clarity consumers are given when creating consents, which could have profound impacts on consumer safety and the reputation of Open Banking across AIS and PIS cases. There could be an increased fraud risk created in the ecosystem due to the absence

of enforceable standards for the PISP side application of consent limits, particularly during the early life of this nascent payment service.

Transaction Risk Indicators' enhancement within the 3.1.10 specifications uplift provides an opportunity for an enriched level of information to be sent to ASPSPs, which could be used to enhance the ability to detected fraud vectors. It however relies on TPPs (which in the absence of TPP standards enforcement and clarification of liability model limits value):

a) Completing all TRI fields, when they are currently not mandated to;
b) Ensuring the data entered is accurate, consistently applied by all TPPs and ultimately usable.

Developing new standards

When considering the development of new standards more generally, a key lesson from Open Banking has been the building out of API end points at significant cost which have since seen little to no use (examples of this include scheduled payments, international payments and offers). No benefit is derived from this and valuable investment could have been prioritised towards other initiatives with clear customer benefit. This reinforces the point that due diligence must be performed to ensure that there is adequate demand and to avoid unnecessary cost.

However, other participants state that the current set of Open Banking standards can meet a range of emerging use cases effectively, and can be adapted or built upon by market participants to meet new commercial use cases. Further standard development at this time is premature before transition to a Future Entity is completed, which can take forward the collective needs of industry in developing further commercial use cases.

QUESTION 2:

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

The variety of APIs used by different players adds complexity and is an obstacle to progressing Open Banking. Part of the concern about implementing APIs is the lack of consistency of implementation across all of the different financial institutions in terms of how their APIs operate within the ecosystem. The current legal framework lacks specific PSD2 API standards and there is a case to be made for EU legislation on payments to include a universal API standard.

A view put forward by some members was that APIs should provide underlying functionality for merchants and PISPs to suggest exemptions, including exemption types. Retailers/PISPs need to be capable of defining the payment context and where exemptions may apply. Most remote payments are performed after the customer has enrolled at the merchant/PISP website or through apps which allow retailer/PISP to enable the appropriate customer experience in payment methods and in the overall customer journey.

Using standardised open APIs for sharing payment and account information will increase efficiency and interoperability, while also driving innovation and increasing adoption of open banking across the financial ecosystem. Having a common language and protocol will make the sharing of payment account data between banks and third-party providers more consistent and easier for developers to build compliant solutions. This will facilitate increased interoperability and enable the harmonization of data protection rules.

Another view put forward was that a decoupled authentication model that works for both payment and data APIs would allow much wider use cases and provide a customer experience which is very close to Apple Pay/Google Pay. A recommendation would be to mandate implementation for banks that already have mobile banking apps. A point raised by some ASPSPs was that if de-coupled authentication was mandated then there also needs to be a liability shift to the TPP on those transactions. Some ASPSPs felt strongly that with no liability shift it would not be reasonable for de-coupled authentication to be mandated.

Ongoing availability and performance of APIs is important to the success of many current Open Banking use cases. Whilst individual ASPSP (either within or outside the scope of the Order) APIs may need to make performance improvements from time to time, some believe the performance of APIs on average across the ecosystem is strong, as evidenced by OBIE data on Open Banking channel performance and parity reporting to the FCA. On that basis, some ASPSPs do not believe broad-based ongoing intervention is required to further improve performance.

It was highlighted that some ASPSPs also act within the ecosystem as a TPP making use of both account information and payments initiation APIs, for example providing an 'account aggregation' proposition and 'pay credit card by open banking' proposition for retail customers. Performance of their Open Banking APIs are sufficient to meet these needs as a TPP.

While PSD2 has set a regulatory framework for availability and performance requirements for Open Banking's regulated functions, the standards and reporting requirements that are currently in place for Open Banking significantly exceed other unilateral payment channels. For example, there is currently a requirement for 99.5% availability (or to match the best performance of direct channels), with all necessary deployment and software fixes needing to take place within the 0.5% of permitted downtime.

Availability/performance statistics from OBIE have largely focused on the CMA9 to date. It has therefore been difficult to determine adherence to standards by other market participants.

Moving from 99.5% to 99.999%

The current Open Banking ecosystem has been designed under PSD2 to match the most performant channels for the services delivered under the CMA Order. For the requirements of the Order it has continued to improve and is now performant at 99.5% (API performance stats - Open Banking) with enhancements to conversion rates referenced by a TPP representative and the OBIE in the IESG minutes from 6th June.

Extending the uses cases beyond the Order will raise the bar in regard to the performance required to match the highest permeant channels under PSD2. For example, card equivalent uses cases such as ecommerce are currently outside the order. To match the most performant channels would require 99.999% availability. To achieve this is a fundamental change in the requires of individual and shared services within the ecosystem, representing a multi-million pound and multi-year investment.

This would include the need for Stand In Processing (STIP) and a level of resilience to meeting consumer and merchant needs that doesn't currently exist and requires a fundamentally different architecture. There are no specifications or guidance on the need for some form of STIP across parties to allow payments to still be made during local or more widespread planned and unplanned outages.

As PIS volumes increase as forecast, and with new higher volume use cases, disruption to service will have an increasingly negative impact on the reputation of Open Banking payments, which may limit uptake by merchants and consumers. (CONFIDENTIAL: As presented in the Payments Expert Panel, earlier this year an ASPSP utilised the STIP process during an unplanned outage lasting over 4 hours. In that time, the VISA STIP process successfully handled c2.5m transactions, worth over £120m of debit card spending with a success rate of over 95%.)

We believe that without comparable performance to cards, uptake of Open Banking payments for all use cases by consumers and merchants may be restricted.

Reliability and reporting

One view put forward is that currently, many AIS/PIS APIs are unreliable in wider use contexts as there are numerous downtimes, even during normal business hours. Most banks do not suffer the same level of downtime for their online banking, mobile banking, or card payment services. Banks should be required to publish the availability ratio in comparison to their other channels e.g. mobile, online, and card. Therefore, any performance and reporting requirements should be applied consistently for all market players.

However, another view put forward is that extensive reporting requirements in place put huge burdens on ASPSPs, which effectively deters new players from entering the market. It may be counterproductive to impose further reporting requirements on ASPSPs. The Payment Services Regulations 2017 ("PSRs") / UK SCA RTS provides the regulatory required level of availability/performance/resilience for ASPSPs and TPPs. Should particular use cases require it, firms would be able to bilaterally agree any higher availability and performance standards.

For future non-regulated functionality, availability and performance standards should be set by market participants on a bilateral or multilateral basis, rather than mandated centrally by the future entity.

Capacity of Faster Payments before NPA

More broadly, there are uncertainties about the capacity of the existing Faster Payments infrastructure to support the increase in transactions associated with material growth of Open Banking payments. Some participants do not believe it is advisable to develop and introduce significant expansions to Open Banking prior to the launch of the New Payments Architecture. Whilst it may be possible to incrementally enhance some of the capabilities available, the Faster Payments infrastructure lacks some of the key functional capabilities to support a large migration of traffic (for example through switching from card payments to A2ART). Moreover, the current Open Banking overlay would require significant scaling, which would require further investment. This is possible, but the costs of this must be shared by all that stand to benefit and be commercially balanced.

QUESTION 3:

What areas would multilateral agreements 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?

The Payments Association believes that a multilateral scheme structure may be required for certain types of transactions. However, it should be on a use case basis e.g. A2ART rather than a blanket

scheme on all activity, with each use case considered within its own right along with a cost benefit/analysis.

Multilateral agreements could be helpful in facilitating the development of an industry-wide liability and dispute model that is based on commercial principles, and has genuine and effective consumer protection built-in.

Multilateral agreements have a role to play in providing Open Banking with common technical infrastructure and standards, and to ensure the overall resilience of the ecosystem. Multilateral agreements would be helpful in developing a robust liability and disputes model and to facilitate commercial sharing of fraud data. Such a multilateral agreement should include a liability framework clearly identifying each participant in the process and defining proportionate liability to the services being provided. Liability should be split among the participant of the systems.

Some participants believe multilateral agreements will be required to support the development of Open Banking for broader use cases, such as A2ART, which may require robust policies and standards (in addition to infrastructure) to provide the necessary customer protections, dispute and chargeback processing, as well as to underpin the liability and commercial models. These should be built directly into the scheme itself, not as overlays.

Buyer/customer protection should be allowed to further develop in a competitive space with the application of minimum liability risk requirements as per the multilateral agreement. Similarly, merchant risk consideration should be allowed to develop in a competitive space.

Differing views among members

However, there are disagreements between participants on whether multilateral agreements should be mandated or optional. Some participants stated that clarity on the intended definition of 'multilateral' would be useful, as it isn't necessarily clear that multilateral agreements on their own, without a supporting scheme-like foundation, are the most appropriate mechanisms given the reliance on all parties in the value change and the lack of detail on new propositions.

There may be space for multilateral agreements in addition to a broad scheme approach. Multilaterals are best utilised where commercial arrangements between entities don't require market standardisation and can instead build from a foundational infrastructure. This is already happening within Open Banking as demonstrated by the premium PIS services offered by some ASPSP and AIS providers.

Some believe multilateral agreements should be mandatory for all participants in A2ART (and FPS/NPA more widely although agreements may be managed separately) and should be installed and managed by entities central to the NPA with the necessary expertise and capacity to oversee and implement the system rules and standards. Some believe A2ART will not be successful if these agreements are optional for participants. The policies and standards for FPS/NPA may not protect customers and support payments sufficiently to encourage adoption; without further policies and standards for retail transactions, this may harm customers and businesses and impair trust in the system.

In this scenario, consideration of how such a set of new agreements should be developed and managed in relation to the broader arrangements that are being developed for the NPA by Pay.UK should therefore be carefully considered.

Some participants highlighted that multilateral agreements may not be able to deliver ubiquity in the core, shared services and principles depended upon by an ecosystem for resilience, fraud protection, performance, and consumer confidence in the highest demanding uses cases. For example, when considering ecommerce PIS, to achieve card scheme levels of availability and security requires uplifts to the core infrastructure. This requires the proliferation of enhanced standards and principles across the ecosystem and would be best achieved through a scheme-like approach. Beyond this, multilaterals can then provide opportunities for competitive, commercial propositions that offer enhanced services to merchants or consumers beyond the core functionality. This could include levels of protection, payment certainty, enhanced levels of data sharing or insight.

Another area of contention is around competition risks associated with multilateral agreements which standardise commercial terms and conditions throughout the industry. With so many suppliers in the ecosystem and so many differing requirements, it is difficult to achieve commercial viability for all.

Distortions and inefficiencies can also be caused by mandating participation for schemes for which there is no market demand, particularly if the burden for funding those schemes falls disproportionately on one type of market participant.

One possible approach could be to permit participation in any multilateral scheme on a voluntary basis, with participants free to determine their own commercial terms. This may be difficult to achieve due to competition concerns.

Role of the Future Entity on multilaterals

Beyond this and more widely, it was highlighted that the Future Entity will need to maintain awareness and monitoring of any services, delivered on a multilateral commercial agreement which could impact the performance, resilience and integrity of the ecosystem and consumer and merchant confidence in it. There needs to be more vetting and due diligence around PSPs, facilitators, and who can integrate and certify with what has been the OBIE.

Many participants stated that there should be a central body (or bodies) able to set and administer participation rules and common standards, a disputes framework and arbitration, and possibly a commercial fee arrangement for ASPSPs. Adherence to these rules and standards should be mandatory and supported by legislation.

Over and above the need for consumer protection and liability, it was highlighted that a range of statutory provision applicable to TPP access to payments accounts will not apply to TPP services outside the scope of the Payment Services Regulations and these will need to be replicated contractually in order to facilitate expansion or development – e.g. provisions around access to and sharing of client data will be necessary, similarly, liability and recovery as between parties (e.g. ASPSPs and TPPs) will need to be addressed. It may be a future consideration to introduce similar protections when developing the strategy for Direct Debit and BACS.

Data sharing

In relation to account information or data sharing, standardisation, including through multilateral agreements, has both costs and benefits which requires evaluation on a case-by-case basis. Some participants advise against being overly prescriptive, at this initial stage of exploration, about how and when outcomes are achieved, on the basis that firms are best placed to understand their customers' needs and design solutions as appropriate. It is likely that demand for new products and functionality will develop organically. Allowing market-led forces to shape the development will enable flexibility in design and foster a more innovative environment.

Developing new propositions

One recommendation is that the industry should have the space to consider further the demand within the market to provide particular use cases, with the JROC process being a springboard to bring these to greater prominence. With the Open Banking Roadmap to conclude shortly, some participants will have greater capacity to engage in commercially focused activity. Where there are clear use cases and clear demand, firms across the ecosystem can work on a commercial basis to create compelling customer propositions. A Future Entity ought to be able to understand and assess where there is clear potential to consider standardisation, which could then be progressed with the agreement of participants.

QUESTION 4:

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

Multilateral agreements exist today in many areas in and outside of Open Banking without regulatory frameworks or intervention. Schemes are necessary to build and maintain ubiquitous platforms off which multilaterals have confidence to exploit commercial opportunity. Just as there are different card network schemes, and where there is more than one, entities like the PCI Standards Council have been established to build out and bring together the standards for the ecosystem. If there is no governance, then market participants, merchants and consumers won't want to invest in something of which they are uncertain.

Blockers

There is a clear differentiation between multilateral agreements on technical standards and process versus unilateral agreements for any commercial models. The biggest blocker is the current lack of a viable commercial model for Open Banking. Commercial negotiations are also hampered by a lack of industry experience, consistency and benchmarking with this kind of multilateral arrangement, as the agreements relate to new and untested propositions.

Where there is a clear benefit in developing multilateral agreements, there do not appear to be any significant barriers. This is demonstrated by the number of existing multilaterals which are delivering services beyond the order, or outside Open Banking. (CONFIDENTIAL: For example, one ASPSP has a commercial contract in place with a data and payments fintech to offer its members the ability to fund new savings accounts with funds held in their non-ASPSP accounts. There are many other AIS and PIS examples similar to this.)

Where there's a scheme or scheme-like structure in place for the development and maintenance of an ecosystem's fundamentals, there is the necessary confidence for an overlaying platform of multilaterals. Within Open Banking, current gaps in the scheme, such as the apportioning of liability throughout the value chain, are not gaps or barriers to multilateral agreements (e.g., where liabilities can be agreed within the contracts).

The central body

There could be a role for a central independent body or management scheme in administering or overseeing multilateral agreements, however some participants state that Open Banking should move away from the current OBIE model for this purpose.

The industry will be mindful of its competition law obligations in developing new standards but for this initiative to be successful, some participants state there will need to be multilateral agreements (including on liability model, commercial fees to be paid, rules on enforcing compliance) developed by the central body, following consultation, that are mandatory and not at risk of subsequent legal challenge (e.g. on competition law grounds) in the courts, however spurious, potentially many years later. Firms cannot plan properly without confidence in the system and legal certainty. To facilitate this, there will need to be appropriate legislative and regulatory support.

However, as stated previously in Question 3, some ASPSPs do believe it should not be a blanket implementation but more based on a use case by case process. There is also the issue of competition law to be considered.

One area of focus for the future Entity, would be the setting of consistent principles on the provision, use and handling of data within the limits of GDPR, whilst any commercial agreements between parties should be administered and governed within the legal framework provided by the contracts. An appropriate governance model would be needed to support a multilateral agreement and to take forward ongoing revision and maintenance to it. Compliance with the agreement and its key terms will require appropriate reporting and monitoring.

The Future Entity should remain responsible for the ongoing interest of the ecosystem and have an appropriate mandate to enforce appropriate controls and measures. Where ubiquitous changes are required, the Future Entity should be directly accountable for administering these and ensuring compliance across all parties in the ecosystem.

QUESTION 5:

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

The main gap that currently exists for Open Banking compared to other payment channels is consumer protection as well as the infrastructure and other elements highlighted in our 'Additional Commentary' section (below) not being built and expected to run on scheme-like availability/processes. Unlike with card payments, there are no legislative provisions in place to offer consumer redress following a merchant failure. The industry's response to a significant merchant failure has not yet been tested.

There has been a very low level of disputes between ASPSPs and TPPs to date, and the current dispute management solution has therefore barely been used. This is expected to change as variable recurring payments are introduced for Open Banking and are more prone to dispute. A more robust disputes and liability model is therefore required. Dispute management must also be considered in the wider context of managing disputes effectively, encompassing chargebacks, refunds, appeals, processing errors and fraud.

This could be done through one single body overseeing the entire process and interfacing with all participants including ASPSPs, TPPs and end-users.

Without agreement from the ecosystem on specific use cases, a scheme can be used to cover a set of principles which help drive a consistent consumer experience. The details of any dispute management, redress and resolution can then be managed within the commercial agreements between parties. This includes arbitration where the contracts provide legal obligations and process for redress.

One view is that the existing dispute management system developed by the OBIE for Open Banking is almost entirely unused by ecosystem participants and is likely to be decommissioned as a result, as it is not providing value and is not suited to potential future use cases, including A2ART payments. This is because the issue was not a technical system but an operational process with a clear liability structure (this is how Visa disputes work on cards).

Consumer protection process

Further development of the Open Banking disputes process (and the related customer protections and liability model) must consider the types of risk associated with each use case. For online A2ART payments, significant further development of the disputes model is required to ensure customers receive equivalent protections to alternative payment methods. However, further thought must also be given to the disputes and liability models for non-A2ART payments given the growth in fraud across Faster Payments vs. the more effective mechanisms in place on card schemes, and similar mechanisms such as Direct Debit.

An effective chargeback, disputes and wider consumer protection system is fundamental to ensuring consumers and merchants are protected and the use of open banking is reliable and can be trusted for both businesses and consumers. The system will require an end-to-end solution, spanning policies, infrastructure and operational mechanisms between stakeholders. Retail use cases comprise the majority of disputes that exist in payments today, with most concentrated in online retail transactions (a key initial use for A2ART), and research shows that consumers are less likely to adopt a payment mechanism if they are not protected. This is therefore critical to driving the uptake of A2ART. The Consumer Protections Act already provides a regulatory framework whereby merchants are held to account for non-provision of goods and services. This needs to be treated very different from fraud.

Established payments systems today, such as the card schemes, have clearly designed and effective chargeback, dispute and customer protection processes and infrastructure to handle the risks associated with retail transactions, underpinned by a liability model that accounts for these risks and adjusts according to the extent of mitigations caried out by participants in the transaction. Consumers and merchants would both benefit from common treatments and processes for

consumer protections across A2ART This approach offers significant value to customers, merchants and the wider ecosystem and help build trust in the payment channels.

As an example, there are four categories of dispute for card transactions. Each contain multiple sub-categories of dispute:

- Consumer disputes, including where goods and services are not received, recurring payments continued after cancellation and counterfeit goods
- Processing errors, such as duplicate transactions, late presentment, invalid PAN or incorrect payment amounts
- Fraud where the customer did not authorise a payment made online or over the phone
- Payments where authorisation was not given or was declined

Each type of dispute has a strict set of criteria that must be met for a chargeback to be issued and to determine which participant holds the liability. These criteria incentivise parties to mitigate risks in a transaction and can be specific to different types of transactions and are based on a complex set of rules and processes that were developed over many years to account for different risks and changes in payment journeys.

Scheme rules then define a set of conditions through which issuers and acquirers can dispute, with liability shifting between parties according to these rules. Where disputes are not settled in pre-arbitration, they will be submitted to a central panel for a final decision based on the evidence provided by participants in the transaction.

The Credit Payment Recovery service for Faster Payments and the Disputes Management Services for Open Banking require significant further development for retail use cases, while chargeback and wider customer protections are not available at all for any use cases. The liability model associated with Open Banking payments is also not well-suited to incentivise the mitigation of risks associated with retail transactions, with liability to customers held by the ASPSP. This is a significant barrier to the adoption of A2ART to purchase goods and services. 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.

Building trust using chargeback and dispute processes

Developing trust in A2ART payments will therefore depend on a significant revision of the existing chargeback and disputes process, with a central arbitration panel and an underpinning liability model, and the introduction of a broader customer protections framework. This is a significant undertaking and should be carried out prior to the growth of A2ART payments to ensure customers are not left unprotected, in conjunction with a commercial model such that participants are able to provide these additional services.

The development of customer protections, chargeback and disputes processes and the associated liability model should look to replicate the successful logic and features of the process established by the card schemes to ensure that risks are managed by participants in each transaction, and to generate trust for consumers and retailers. This also will ensure that customer protections are aligned across payment options to minimise consumer harm and to prevent merchants being faced with multiple different processes.

One participant highlighted that there needs to be infrastructure for different types of transaction, and different categories of PSPS and ASPs, and more validation on different types of transaction. With A2A transactions, there should be very little disputes. This could possibly be done with some form of blockchain, where individual transactions can be reviewed and disputed similar to card payments. There needs to be a platform where every single transaction is clearly identifying the different actors, whether it be a PISP or ASP transaction, and not just vanilla A to B transactions. All the different entities that are involved, identified and validated as part of that process, and whether they have the privileges and the capabilities to do those types of transactions, should form part of that.

QUESTION 6:

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

As Open Banking expands beyond the order with more AIS and PIS uses cases and users, this will place greater systemic importance on the shared infrastructure for the economy. Currently, if there was a significant volume of ecommerce purchases flowing through the Open Banking ecosystem and there was a prolonged outage of the Open Banking directory, or a security breach, it is not clear how it would be handled. To date there is not a clear strategy to address this. One example given was the Open Banking Directory outage in August, which if it had extended much further, could have led to an outage of both Open Banking and Confirmation of Payee (CoP) services. If that had happened, it's not clear how it would have been centrally managed and communicated to parties and consumers as part of a Serious Incident Management Response.

As another example, a similar crisis was a huge doubling of the amount under Faster Payments of push payment fraud, that was then retrospectively dealt with. Learning about how that was resolved would be a good starting point.

Dealing with concentration risk

Open Banking works on a shared directory and security model, which creates a concentration risk that needs to be considered for crisis management, including the communications and incident management support plans around it. At ecosystem level, there is more to be done to mitigate the concentration risk of the shared infrastructure. A crisis management strategy and plan should be created to cover those systemically critical service, akin to those used in the card ecosystem, to support the growth of and national reliance on the Open Banking ecosystem.

Requirements for disaster or crisis management should be in line with similar arrangements for financial services firms as set out by sector regulators, to which many participants are already subject. Where wider industry coordination is required, an appropriate industry body should be given this remit. Regulators should then take note of any risks which cannot be mitigated through ordinary industry cooperation.

A variety of views across the ecosystem

Care needs to be taken not to create an excessive regulatory burden, given other parallel regulatory measures that are being developed regarding operational resilience in the provision of payment services. The SWG should cooperate with other regulators to avoid duplication with other initiatives, and to avoid unnecessary compliance costs and operational burdens being placed on Open Banking market participants.

One view put forward was that ASPSP payment resilience is already subject to a high degree of scrutiny. By contrast, only limited requirements exist regarding TPP resilience. Where central industry functions or processes are provided and supported by OBIE, points of failure continue to exist - in August there was a failure with the Open Banking Directory that took down the service for a significant period. Resilience requirements should be consistently applied to all types of market participants.

As the growth of Open Banking payments accelerates, it may become necessary for regulators to consider whether firms, including sizeable TPPs, could be considered systemically important for the UK payments infrastructure. Given the risks related to the sharing of large amounts of customer data via APIs, it is important that TPPs storing and processing customer data take steps to ensure that it is appropriately protected and that response plans are in place to ensure appropriate management of any data breaches.

Some participants stated that it would be useful if this question provided more clarity on the scope/scenarios considered, given the potential range of scenarios this could cover. All organisations have their own crisis plans across their business functions, including Open Banking. To that end, individual ASPSPs and TPPs should not need any external direction or oversight.

QUESTION 7:

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.

Our members had a wide variety of views regarding the use of trust markets and other tools to build trust, and whether this will lead to greater adoption, and this is reflected in this section.

Some participants stated that consumers have not flocked to Open Banking because of the fear of their private data being stolen or compromised, and trust marks would be a good way to improve customer trust in and awareness of Open Banking.

However, other participants believe that there is no evidence of a lack of trust, but that the slow growth of Open Banking to date results from a lack of consumer awareness, and not enough incentive to change consumer behaviour. The number of users continues to increase month on month across the ecosystem, most noticeably within PIS. (CONFIDENTIAL: one ASPSP current forecast predicts a monthly growth of 3% for AIS volumes and 7.5% for PIS; with the impact of VRP sweeping yet to be established.)

The priorities for building trust and adoption

The most immediate priority to strengthen users' trust in open banking is the development of the customer protections, disputes and liability models. Creating the right protections and incentives for stakeholders within A2ART is crucial for driving its adoption against well-established alternatives. Introducing customer protections (including chargeback and disputes processes) and a liability model that is well-suited to retail transactions is critical to protect customers and establish consumers' trust and willingness to use it as a payment option.

The introduction of a commercial model (across all payment categories, not just A2ART) that recognises the full costs and value of the system (including the customer protections and liability

model) will ensure that there is a fair and sustainable return for all participants that promotes the right incentives for the functioning of and investment into the system. This should enable benefits across a balanced ecosystem, including for merchants who should benefit from additional ways to pay, enhanced journeys, the opportunity to improve cash flow, and improved checkout completion.

It may be more a lack of awareness or compelling products that has limited consumer uptake in Open Banking. Open Banking is a technical solution that isn't widely understood or resonates with consumers at large. Better promotion will come by scaled use cases backed by significant, recognised and trusted brands. Perceived consumer value in the use cases is likely to be such that how it's technically executed is irrelevant to consumers. Going forward it will be vital that trust is maintained, hence the need for clear, consistent journeys and consumer buyer protections and fraud, and a reliable, resilient core infrastructure.

The maturity of the payments market in the UK, and the ease with which it is possible to make payments using other established methods, has made it difficult for Open Banking account-to-account (A2A) transactions to gain market traction. Some believe that to change customer behaviour requires TPPs and merchants to invest in a targeted marketing campaign to educate consumers on Open Banking, however most others believe that this investment is not justified by Open Banking's commercial upside under the current model.

Trust marks

With circa 6 million consumers using Open Banking, where there are propositions that are valuable and offer benefit to the payment system user, the suggestion of a voluntary 'Trust Mark' being created for Open Banking payments was put forward. Some supporting quotes given include the use of the contactless symbol which has worked well, as did the generic 'Cards Accepted' statement in the early days of card payments. Trust is linked to the availability of payment protection and ease of use. One participant stated that it would be beneficial from a merchant perspective to put something in place to highlight that, similar to the five-step logo to authorise push payments. There could be some sort of moniker of Open Banking to show that vendors have gone through the process, as with different levels for PCI for example, whether a Level One processor or merchant, down to Level Five.

Any further work to promote the adoption of A2ART should be based on consumer research and should recognise the value of a standardised approach across the system. For example, the identity and brand of Open Banking today is confusing for customers when compared to established retail payment options such as credit and debit cards and PayPal. There is inconsistency in its presentation across different use cases, and a lack of awareness of the difference to other payment options.

Sharing the cost of building trust

Consideration must therefore be given to the branding and customer awareness of any A2ART payment option, such as through trust marks, such that customers know the protections available. However, it is important that any costs associated with this common identity are shared between all participants that stand to benefit from its creation. Moreover, this common identity should not be introduced ahead of the development of trust in Open Banking through customer protections and the disputes and liability models described above to avoid confusion and potential harm for consumers.

Some participants state it is less clear that Account Information Sharing by Open Banking would merit from an identity or brand. Instead, the priority here is on ensuring that data is appropriately used and protected. Customers are willing to share their information with organisations that they trust, to receive services in which they can see clear value.

Conclusions

However, the OBIE has conducted a number of investigations on this topic. By doing so, the OBIE demonstrated that there is no real value offered from a trust mark. This was reflected in the CMA deciding to exclude trust marks from the current roadmap. Some participants state that the lack of a trust mark is unlikely to impede further uptake or consumer trust in Open Banking. Trust marks often take time to gain consumer awareness, understanding and trust. It would also require a consistent application of the trust mark to ensure consumers experience the level of protection expected from it between merchants/PISPs. Trust marks can also be exploited by fraudsters, giving consumers a false level of reassurance.

More widely, ensuring that all participants are fairly charged for the benefits they derive from the system and take on appropriate risks through the distribution of liability, will also better incentivise acquirers and payment processors to support A2ART payments through their payment gateways, reducing the operational burden on retailers. As such, key stakeholders throughout the value chain will be aligned to encourage its adoption.

QUESTION 8:

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

Some participants believe that for the current, supported uses cases in the Order, there is insufficient evidence that further tools are necessary. There have been cases where clarification has been sought on application of GDPR in the context of Open Banking data exchange, treatment, and onward sharing of data, but this hasn't prevented the uptake of Open Banking by circa 6 million users.

Consumer understanding and awareness

This should be kept under review by the Future Entity tasked with monitoring standards. Individual firms can act by updating customer information and guidance, including FAQs. Customers will be drawn to specific value propositions, which then require use of open banking connections, rather than being drawn to use open banking in and of itself. It is too early to fully understand how customers will interact with variable recurring payments consents, but the industry will need to be responsive should any adverse developments arise.

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, it is increasing awareness of Open Banking would not 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. Before that can occur, a viable commercial model is needed before market participants can justify investments in such new value propositions .

Consent management

In terms of consent management, providing consent for one-time payments is a straightforward part of the transaction process and is comparable to what consumers are used to with other payment channels. Therefore, no additional consumer guidance is needed for this type of payment.

By contrast, for sweeping payment consents and for AIS consents, additional user guidance could be helpful for consumer protection purposes and be displayed in the same way as direct debit e.g. in the app menu or navigation systems. Some participants also believe it is important for consumers to have an email or text confirmation for the same.

One participant stated that principally, there needs to be understanding of who the regulator scheme is, and to what level and category the different actors have been certified. Guidance around areas such as confirmation of payee for authorised push payments and associated scams would be helpful. This would not only give confidence in the security of Open Banking but also can have the other effect of promoting it.

For future, more complex uses cases that share broader data and different data, greater clarity may be needed on GDPR rules but this depends on the use case and data. For example, UKF's Enhanced data sharing proposition for enhancing APP detection and prevention relies on the sharing and matching of customer data between institutions for fraud prevention purposes. With the breadth of data being considered for the effectiveness going beyond traditional levels of detail, a critical question being considered is what can still be considered appropriate under GDPR. This is a key question to resolve for this initiative progress. This illustrates the need for guidance to be provided on a use case basis as opposed to by a single generalised policy from a central body.

QUESTION 9:

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)

All firms participating in Open Banking are required to adhere to current data sharing standards as set out by PSD2 requirements. Customers have access to information about onward sharing and there have been no customer issues arising that our members are aware of from Open Banking data sharing to date.

A regulatory framework for data protection already exists in GDPR. Once a customer has made the decision to share access to their data and that data has been provided, there is little that an ASPSP can do in terms of how that data is then used or shared with other parties. It was raised by some that not all TPPs are explicitly when gaining consent explaining how data will be used. Guidance could be published to ensure better cross-industry standards are adhered to.

Every actor in a value exchange needs to be held to the same standards and bar for consent management across AIS and PIS journeys. This could be via a single standard for sharing consents and consent management, applicable to every party in the value chain. Currently, this would be covered via CEG requirements, however, these are only mandated to the CMA9.

The CMA9 are only one part of the overall value chain and removed from the initial presentation of the consent parameter to consumers. The current lack of enforcement for other parties to adhere to

the same guidelines leads to inconsistent and potentially detrimental consumer experiences and outcomes.

There needs to be some sort of standard around who can effectively touch account information, and who is allowed to touch, store and forward Open Banking related data. Again the example of the PCI Council was given as a possible model to follow.

QUESTION 10:

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?

Within the broad context of Open Banking, different actors and roles within the ecosystem need to be consistently defined with a clear set of liabilities and responsibilities. All actors need a common set of responsibilities and requirements for the adherence to scheme standards. Clarity on liability, dispute management, crisis resolution and handling of exceptional circumstances are the ways these can be achieved.

Clarity and credentials

There needs to be a clear set of policies and procedures around all of the different actors. Understanding who is actually in the ecosystem, and who is going to have access to their data, and in which environment, such as shared data centres or in-house data centres. Data maps and data journeys should enable the tagging of information, so that ecosystem players can identify that transaction all the way through and see who has touched it.

Ecosystem players can only be accepted or be validated for receiving data as long as they provide credentials that are recognised, and those credentials are then linked to specific privileges and capabilities. Those privileges are aligned to the capabilities for which they have been certified. It needs categorisation based on the individual transaction. For more complex transactions, they can be performed by the players that have the capabilities and the requirements involved, and environments that are suitable for doing more complex transactions where more data is shared.

An open participant register should be maintained where anyone could go and validate information, for instance checking if a TPP is authorised or not. A multilateral framework can facilitate the identifying and defining all the participants in the framework.

Going forward, where required the single authority should align all TPPs and ASPSPs on a mandated basis for all parties in the ecosystem.

However, many of the roles and responsibilities of key actors are defined within existing regulation. It is perhaps too early in the process to say whether further consideration of this topic is required, other than that it ought to be borne in mind by the Committee in considering the design, role and functions of any Future Entity such that they are clearly demarked and understood vis-à-vis existing bodies.

QUESTION 11:

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.

OBIE currently provides several central functions that are needed for Open Banking's successful operation. This includes: (i) standards maintenance, (ii) roadmap and standards evolution, (iii) central technical services, (iv) Open Banking Directory Management, and (v) COP certificates service using a related model and methodology.

There is a need for a scheme to deliver and enforce a ubiquity of standards for the development and maintenance of core and shared ecosystem services. The core capabilities requiring a centralised governance through the Future Entity include ecosystem strategy and roadmap, standards development, centralised communication, ecosystem monitoring, alerting and incident management, data management and IT operations. Provision of these could take a number of models. Providing through one centralised entity is only one option. It's possible for there to be a competitive market for the provision of capabilities and services.

Central vs. distributed services

Technical, certification, governance and monitoring functions benefit from being centrally provided, however these could potentially be divorced from the technical functions. Open Banking as a central body has worked well for standard implementation but for example has not been as effective in improving the consistency and in some cases, the reliability of APIs. It would make more sense to have distributed services, for instance dispute management and directory services could be managed separately. MI reporting and multilateral framework and oversight controls should be managed together in one entity.

Having the ability to validate individual actors that are performing a function or have access to that data would be beneficial. It would include entity validation in real time, and also retrospective, as in the example of disputes, and being able to see what's happened for any given transaction or query, or sharing of data. For more complex transactions, a governing body that can basically certify, provide documentation and testing tools and provision, and the ability to certify those different actors, is needed.

Likewise, the development of standards could be delivered outside the future entity. Beyond any shared services requiring ubiquity across the ecosystem, where existing multilateral agreements exist, standards are agreed for the purposes of that solution, within that competitive space.

Monitoring

There is also a question as to why Open Banking requires a monitoring function different to any other payment method in the UK, where there are established processes in place to report to regulators if there is an incident. The governance model applied to other payments channels could be used as guide. These are regulated by the FCA and the PRS without the need for a separate enforcement body.

With the CMA Roadmap drawing to conclusion, there is a need to move to a more sustainable, commercially-led and efficient footing to serve the industry's present and evolving needs. The status quo cannot, and should not, continue into the "interim state" for the OBIE. A future entity should be:

- Independently led and accountable
- Adequately resourced
- Dedicated to serving the interests of consumers and SMEs
- Sustainable and adaptable to future ecosystem needs
- Highly efficient

To provide a model that can take forward the further development of open banking in the UK, as well as an future industry or regulatory initiatives, it is essential that:

- Funding is equitable across all participants
- Liabilities are appropriately capped and shared
- Scope of services and their cost is clear and subject to regular review

The existing functions of the OBIE could be undertaken by either the Future Entity, another industry body or outsourced to the commercial market. A full review of the capabilities provided by the OBIE today should consider whether:

1) They are needed at all
2) If needed, can they be provided in a more efficient or effective way
3) If they need to be transferred to a future entity
4) If they serve an oversight or monitoring function that is no longer required, or could be transferred to a sector regulator

For example, in relation to the OB Directory service, alternative models for identity verification could be more efficient, operate at lower cost and with better distribution of risk. In relation to monitoring, there are many examples of monitoring and oversight approaches used successfully by sector regulators that would properly allow for the ongoing oversight of Open Banking, without undue overhead, cost or governance constraining a future entity.

Commercial foundations

In addition to the existing functions of the OBIE, there is a need for industry to be able to develop new propositions on a commercially-led footing. A2A Retail Transactions could be an early example of this, where the capability to establish and maintain a multilateral agreement, funded by participants, alongside any supporting revision to standards would be required.

For those that do not wish to participate in further developments, the Future Entity needs to be able to support a set of standards and arrangements that maintain regulatory compliance, while allowing others to move beyond this.

A view expressed was that many of the existing services offered by OBIE could/should be now provided by the market. It was felt that this would offer a more commercial and dynamic market. The simile given was of a child learning to a ride a bicycle in that stabilisers maybe be required in the early days but not later when the child knows how to ride. Open Banking has matured and the stabilisers and some of the OBIE functionality currently offered as services can now best be delivered by the market. It was felt innovation designed from the centre does not always work best; innovation must be allowed to develop and this is generally agreed is best done though allowing the market to offer the services.

ADDITIONAL COMMENTARY:

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

Strategy

It is not clear what the overall strategy is beyond the Order. Within the Order, the strategy was clear; promoting competition in current accounts. What are the outcomes looking to be achieved that will determine the Open Banking Plus roadmap? This will help ID requirements, the nature of the scheme and current gaps.

One participant recommended a formal clarification on the strategy and what it is looking to achieve backed by data, in the same way there was for the original CMA order. It referenced the CMA market investigation report that identified seven adverse market effects that needed to be addressed, e.g., the adverse effects on competition (AECs). These framed the outcomes of the CMA order and subsequent roadmap. This will be required before appropriate outcomes can be identified.

Funding

Additionally, the funding model for the ecosystem has not been discussed in the first round of sprints but it is fundamental in the future model for Open Banking. The funding for delivering the enhancements to the shared infrastructure and ongoing running and maintenance needs to be shared appropriately across actors in the value chain. The original Order was funded solely by the CMA9. Continuing to put this level of demand on the CMA9 will distort any future commerciality in Open Banking, relying on a small subset is subsiding the benefits realised by others. As an example, it will not be possible to extend use of Open Banking APIs for enhanced fraud data sharing under the current model where the CMA9 carry the cost and risk of that service.

Some ASPSPs highlight that there needs to be a commercial value to ASPSPs in order to make A2A payments sustainable in the long term. It's essential for ASPSPs to continue to operate in the ecosystem and provide commercially sustainable current accounts to consumers. (CONFIDENTIAL: This is already a loss-making service for some participants due to the range and levels of service needed to provide in order to allow members to operate them).

Expanding the uses cases of A2A would need to be sustainably funded without breaking the commercial model (i.e., to protect free in credit banking). For example, to offer A2A payments for ecommerce, there must be a way for merchants and PISPs as beneficiaries to pay for the service and infrastructure that underpins it by ASPSPs.

Beyond Open Banking

The questions across this first sprint have not directly considered the broader development of A2A payments, outside of Open Banking. It should be acknowledged that whilst Open Banking is likely to be a significant driver in A2A retail transactions, there may be other solutions and mechanisms coming to market (e.g., PayByBank) as well as the impact of Pay.UK's NPA. For the health of the ecosystem, Open Banking payments will need to offer consumers and merchants a competitive proposition. The committee should consider if there are opportunities to align to and influence the broader developments across A2ART in order to provide a clear consumer experience or competitive point of difference.

One participant stated that it is important for the Committee to view further developments of Open Banking payments in the context of overarching regulatory and industry priorities, including the development of the NPA by Pay.UK, the market review of cards, and the need to ensure appropriate consumer protections and protect from fraud however a customer chooses to pay. To do this effectively, Open Banking cannot be considered in isolation.

To unlock the desired outcomes and build consumer trust, the future of Open Banking and A2ART should include common standards of consumer protection, including protection from fraud (including APP), the ability for consumers to raise disputes/chargebacks, and merchants to benefit from additional ways to pay, enhanced journeys and improved checkout completion. The ecosystem should be underpinned by a balanced and sustainable commercial model, in the style of interchange, which has legal certainty through legislative and regulatory support.

Data sharing

The industry is already progressing new opportunities in data sharing (e.g., in fraud and digital identity). Data sharing will progress, and consumer outcomes be realized, where incentives exist for all parties to participate in the market. Where there exists a commercial opportunity, both TPPs and ASPSPs will be motivated to work together to identify the opportunity and to find solutions. Allowing the market to develop these solutions will tend to result in more efficient, sustainable and cost-effective outcomes.

Smart data

It is also important to consider the wider range of potential 'smart data' solutions outside of financial services, to be enabled by the Data Protection and Digital Information Bill, that can expand data sharing to realise benefits cross-industry, as well as unlocking access to government-held data, which could deliver greater consumer benefit.

It should be noted that some potential future outcomes could be realised through alternative solutions to Open Banking. The Committee should be open to firms taking a variety of approaches in order to achieve expected outcomes. The best customer outcomes will be achieved through an ecosystem that allows for competition between business models as well as between providers. For the customer to have the widest choice of products, services, and business models, it may not be necessary for all firms to provide third party access beyond existing regulatory requirements.

Charities

The role of charities in the ecosystem also needs to be considered in relation to the above issues. Explorations are ongoing with some ecosystem participants about how micro donation solutions can fit within Open Banking, and still maintain key principles of micro donations and generate more income for charities and not just replace existing value. From a governance perspective, every penny which is donated via Open Banking must be guaranteed to reach the nominated charity or charities.

Duplication

Some participants note that some of the questions, in particular Question 1, were covered in depth in other sprints, and expect far more detailed responses to have been received by SWG in regard to gaps in standards etc.

Comparisons with the 50-year track record of scheme payments

A2A payments have been designed and PSD2 required standards that met other direct channels i.e., web/app. They have not been required to be of the resilience and structure of a scheme-style card payment. To that end, the technical capability, operational support, consumer experience, protections, and legal frameworks have been developed over 50 years for real-time POS and ecommerce transactions.

A2A payments are designed and architected for different use cases that have different requirements around time and sensitivities. The uplifting of ASPSPs to enable a scheme-like capability is a very significant uplift that will take time and significant cost. In the view of the Payments Association, this is unrealistic to achieve in a short period of time. Given that A2A payments are currently free to the payment user, any requirement to upgrade A2A to the same resilience as a scheme may challenge ASPSPs to continue to offer their existing free/low fee current accounts.

As part of the response, the Payments Association would recognise that the NPA is due to develop and specify a set of standards for A2A payments, and this may have a significant impact on the overall responses.

The Payments Association would highlight the work that is currently being undertaken by SPAA in the EU, and would highlight the need to understand in more detail this work to see what learnings and structures could be copied in the UK market.

Overall though we would additionally caveat that multiple participants made the point that a two-week time period for submissions was insufficient time to gather relevant information, formulate comprehensive responses and submit responses in a timely manner given normal business operations. The Payments Association's 180+ membership demonstrates the scale of coordination needed to gather input and whilst we had a good number of respondents we are aware that with greater time an even larger number of respondents would have contributed.

For more information please contact Tom Brewin, Head of Projects, The Payments Association, tom.brewin@thepaymentsassociation.org or see our Project Open Banking details at our web site, https://thepaymentsassociation.org/portfolio/project-open-banking/.