



**Electronic Money Association**

Crescent House

5 The Crescent

Surbiton

Surrey

KT6 4BN

United Kingdom

Telephone: +44 (0) 20 8399 2066

Facsimile: +44 (0) 870 762 5063

[www.e-ma.org](http://www.e-ma.org)

Laura Mountford  
Payments Landscape Review  
Payments and Fintech Team  
HM Treasury  
1 Horse Guards Road  
SW1A 2HQ

20 October 2020

Dear Laura

**Re: EMA response to HMT Payments Landscape Review Call for Evidence**

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. They also include a growing number of Payment Initiation Service Providers (PISPs). The EMA sits on OBIE's Implementation Entity Steering Group and participates in European initiatives under the aegis of the Euro Retail Payment Board. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our concerns.

Yours sincerely

Dr Thaer Sabri  
Chief Executive Officer  
Electronic Money Association

## EMA response to consultation

### **Question 1: To what extent do you consider that the government's objective that UK payments networks operate for the benefit of end users has been met?**

We welcome the actions taken so far; both strategic interventions around the governance of UK payment systems, regulatory changes, and the support of competition measures such as the creation of the Open Banking ecosystem. This has resulted in a growing and vibrant financial technology market in the UK with regular new entrants and innovative solutions.

Although major strides have been made towards ensuring that payment networks operate for the benefits of end-users, at least in terms of the governance and strategy objectives for the UK payment systems, there are a number of operational adjustments that could improve transparency and ensure that decision-making continues to involve all interested stakeholders. We have set these out under Q2. As Pay.UK's responsibilities grow, and the New Payments Architecture (NPA) evolves to underpin the UK's payment networks, the importance of transparency and access to Pay.UK's governance and operating structure will become paramount for all end users.

### **Question 2: What do you think industry, regulators and government should do in order to further ensure that UK payments networks operate for the benefit of end users?**

#### *Governance and transparency of payment schemes*

Although major strides have been made in the governance and strategy objectives for the UK payment systems, there are a number of operational adjustments that could improve transparency and ensure that decision-making continues to involve all interested stakeholders:

1. Further steps should be taken to ensure the meaningful participation of non-bank PSPs and PSP representatives in decision-making on payments. The membership of Pay.UK's End User Council and Participant Council should be reviewed on a regular basis, and not remain static, as different stakeholders will bring different interests to the table, and the right balance of stakeholder representation will need to change over a period of time.
2. Many of Pay.UK's workstreams and processes lack transparency, and are difficult to access for stakeholders that represent smaller PSPs and industry bodies such as the EMA. The EMA represents a large number of smaller organisations that do not have the resources to track or contribute to Pay.UK work, but for whom these initiatives are very important, many participating in-directly with the payment schemes operated by Pay.UK. The current Pay.UK contractual and confidentiality arrangements restricts the EMA from actively participating in Working Groups run by Pay.UK.

#### *Timing of initiatives*

The development of the New Payment Architecture (NPA) and Open Finance will take several years of concerted industry and government effort to achieve. We therefore propose the Government would be well advised to invest resources in ensuring the proper and full implementation of existing changes, including if necessary targeted rule changes, as well as initiatives that are already in train, such as Open Finance and the NPA, rather than pursuing new ambitious projects for the payments industry.

**Question 3: To what extent do you consider the government's objective for a UK payments industry that promotes and develops new and existing payments networks has been met?**

*New Payments Architecture*

The EMA supports any efforts to improve accessibility to payment systems for new participants: improving competition and having simpler onboarding processes will allow a wider range of businesses to have access, and can benefit and advance the UK's payment ecosystem. We therefore welcome the vision for the New Payments Architecture (NPA) which will simplify the set-up for smaller participants, standardise payment message formatting, and provide the ability to send and receive a number of different payment 'types' within the same system.

The NPA will also reduce complexity from a technical maintenance perspective, and in particular for smaller firms or firms without historical connections to the system. Allowing newer market participants to have easy access to a central payments infrastructure, and establishing a platform that supports all payments types will be of considerable advantage to the fintech sector and the payments industry as a whole.

The layered approach of the NPA will foster competition, innovation and ease of access to new entrants. The NPA aims to provide the basis for future payment systems infrastructure to be more agile and flexible than what exists today whilst maintaining security, stability and resilience. Where there is demand, there should be the ability to launch new services more quickly. This approach is proven in other industries, such as telecommunications, and is being adopted by other countries as they transform their payment systems.

However it is difficult to comment on whether the Government's objective has been met, as the NPA remains to be completed, and there is very little visibility for the wider payments ecosystem over developments since the vision for the NPA was published in the Payment Strategy Forum (PSF) Report (2017). Pay.UK's Dec 2019 questionnaire on understanding stakeholders' views on the NPA scope ambition reveals that the design and implementation of the NPA is still very much under debate, three years after the PSF set out its recommendations, yet the wider payments ecosystem has had a very limited visibility of, or opportunity to participate in those discussions.

The EMA is concerned that there is a risk that the scope of the envisaged NPA is reduced over time, due to time and cost pressures for incumbent BACS and FPS scheme participants. The two-tier payments infrastructure this would inevitably create, with potentially Faster Payments using the NPA and BACS on legacy systems, will restrict the speed and scale of innovation in the UK payments market. If the NPA simply becomes a like-for-like replacement of BACS/FPS functionality, legacy technical, operational, and competition issues may be introduced into the NPA ecosystem, and the government's objectives will certainly not be met.

We therefore urge HMT to ensure the creation of a payments architecture that is open, fit for purpose, and drives competition and innovation in the UK payments market, and not an approach that merely upgrades existing legacy systems such as BACS and Faster Payments.

### *Support for new payment services firms that employ new technologies or business models*

We believe the government has moved some way towards achieving the objective of developing a UK payments industry that promotes and develops new and existing payments networks. The regulatory framework for e-money institutions has allowed a wide variety of different business models and products to develop. This has given consumers access to a much wider range of financial products that address particular use cases and customer demand, driving down costs for consumers.

It is therefore crucial that the Government continues to embrace a proportionate, risk-based approach towards the e-money and payments sector as it is still relatively new. The current activity-based regulatory framework has allowed firms to offer services and products that address particular use cases and customer demand, without taking on the risk associated with the offering of credit. Using regulatory tools or requirements designed for credit institutions may therefore not always be appropriate for e-money institutions, as their business model, products and risk profiles differ from major high street banks, or investment funds.

### *Open Banking*

The CMA Order has helped to facilitate the beginnings of Open Banking in the UK. However it is too early to determine whether the resulting ecosystem has met the Government's objectives. This is particularly true for payment initiation services where commercial propositions are just beginning to emerge in the market, and the industry is still in its infancy.

We urge HMT to consider our suggestions in our responses to Q4 where we set out further steps that could be taken to improve the success of Open Banking, and ensure that the ecosystem can support a diverse range of payment options where there is clear market demand.

### **Question 4: What do you think industry, regulators and government should do in order to further promote and develop new and existing payments networks?**

The development of the New Payment Architecture (NPA) and Open Finance will take several years of concerted industry and government effort to achieve. We therefore suggest the Government should invest resources in ensuring the proper and full implementation of existing changes, as well as initiatives that are already in train, such as Open Finance and the NPA, rather than pursuing new ambitious projects for the payments industry.

### *New Payments Architecture:*

As set out in the PSF Strategy (2017) and the PSR's 2017 Direction to Pay.UK, the replacement of the BACS and Faster Payments (FPS) clearing and settlement layer is at the heart of the NPA. However, the scale and complexity of upgrading these payment schemes means there is significant risk that the scope of the NPA is reduced over time due to time and cost pressures for incumbent scheme participants. The two-tier payments

infrastructure this would inevitably create, with Faster Payments using the NPA, and BACS on legacy systems, will restrict the speed and scale of innovation in the UK payments market.

Curtailling the scope of the NPA would also likely increase the risk that the NPA becomes a like-for-like replacement of BACS/FPS functionality which may introduce legacy competition issues into the NPA ecosystem. For example, connectivity options to FPS currently attract significant setup and on-going operational costs, for participants who are required to establish a direct physical connection to the FPS CIP or route via an intermediary. The FPS CIP also requires participants to access and pay for transaction data as an ancillary service to core transaction processing, via a separate technical connection.

The above examples illustrate that historical technical design decisions made regarding FPS and implemented by the FPS CIP have led to down-stream competition issues by placing cost barriers for smaller payment providers entering and participating in the ecosystem.

In order to mitigate against the risk that the NPA, and its operation by the CIP, perpetuates these competition risks we urge HMT to ensure that the NPA CIP, and NPA technical scope and design will create a payments architecture that is open, fit for purpose, and drives competition and innovation in the UK payments market.

#### *Open Banking:*

As discussed under Q3, it is too early to determine whether the Open Banking ecosystem has met the Government's objectives, particularly for payment initiation services where commercial propositions are just beginning to emerge in the market. Below we set out further steps that could be taken to improve the success of Open Banking, and ensure that the ecosystem can support a diverse range of payment options where there is clear market demand.

#### Regulatory framework:

##### PSRs

- Wide definition of a "payment account" which is accessible online: Some new market entrants and smaller PSPs that provide payment accounts are often disproportionately affected by the need to provide third party access to those accounts under the PSRs. In many cases they face considerable costs and challenges in providing access, despite being able to show there is no demand at all from TPPs to access their accounts due to their business model or niche propositions. There is an opportunity to introduce thresholds (volume of payment accounts, volume of transactions, etc.) below which PSPs could launch and operate payment services without having to provide TPP access to payment accounts. This could also be coupled with an exemption process for those PSPs whose payment services and accounts see no demand from TPPs for access.
- Assess and review the definition of account information service: the definition of account information services should not restrict AISPs to have to 'provide' consolidated account information to the payment service user that they have accessed. This restricts the services that AISPs can offer, and will ultimately affect innovation in the market.

- Regulatory perimeter: PISPs should be able to access payment account data in order to manage their payment risk prior to initiating a transaction even if they don't intend to offer AIS products.
- Consult publicly on how the PSR's regulatory initiatives of the Contingent Reimbursement Model (CRM), and Confirmation of Payee (CoP) should be treated in open banking customer journeys. In the absence of any formal policy decision-making process, the implementation of both initiatives by ASPSPs may have an adverse effect on the success of open banking and open finance by making AIS and PIS services cumbersome and unattractive to customers.

#### MLRs:

- Remove AISPs from the scope of AML legislation. If remaining in scope, ensure that expectations and provision are proportionate to the risk. AIS products involve no initiation or execution of transactions, providers cannot influence any kind of activity that could give rise to money laundering and are simply independent observers of the activities undertaken by their clients. Without specific consent and authority, AIS providers are not entitled to review their customers' data, which originate elsewhere, and to do so would be an abuse of their customers' expectations of trust and confidentiality. Given that all financial services related data will have already been reviewed and be subject to monitoring and reporting obligations by the relevant originating service provider, this reinforces the absence of a nexus between an AIS service and anti-money laundering risk mitigation objectives.

#### UK-RTS

- HMT should review the UK-RTS and consider enabling TPPs to operate continuous, unattended access to account information, without the need for the customer to provide authentication to the bank every 90 days.

#### Future:

- Open Banking Roadmap: press ahead, especially with variable recurring payments (to enable PIS to better compete with card on file payments and direct debits where there is market demand)
- Open Banking Future Governance: the future governance model for taking forward the open banking standards and assets (OB Directory, and DMS) once the OBIE has completed its mandate under the CMA Order should be resolved as a matter of urgency so as to provide a degree of certainty to the Open Banking ecosystem. It is important that governance remains available to TPPs, and HMT oversight should ensure that it is not dominated by ASPSP interests.
- There is a lack of structured consultation and communication with the TPP community on key developments that will affect TPPs and their end-users out with the Open Banking Implementation Entity. There is also appears to be a lack of coordination in the oversight of Open Banking between FCA, PSR, OBIE and CMA.
- Explore and fully develop a digital identity strategy for open finance: A single electronic identity that could be used by UK consumers and businesses for access to all regulated financial services will reduce friction and improve adoption of open banking services, and should form the foundation of any open finance initiative.
- Authentication of payment service users: PISPs cannot offer innovative products that are adapted for new channels and devices e.g. voice-enabled payments, payments at

Point-of-Sale terminals, or payments using a wrist watch - when customer authentication journeys are restricted to the 'redirection' authentication model as is currently the case in the UK.

Supervision of ASPSP API performance and implementation:

- The FCA currently does not have sufficient resources dedicated to the supervision of Open banking to ensure it will be a success. A permanent dedicated open banking supervision team should be established with the appropriate levels of expertise and experience.
- The level of support and status updates provided by the major retail banks for their dedicated interfaces (APIs) should be equivalent to the support provided for their own online channels (as required under SCA-RTS Article 32(1)). This is often not the case, and should be monitored and enforced against. It is imperative that a 'two-tier' API ecosystem does not evolve where open banking API performance and operational resilience are sub-optimal in comparison to ASPSPs commercial API services. The poor performance of ASPSPs' open banking API infrastructures for TPPs can already be seen to be providing ASPSPs with an advantage when they decide to provide AIS/PIS services. The ability for ASPSPs to create services based on well performing APIs (or internal services), which are not available to external TPPs, will suppress the TPP ecosystem.
- Transparent enforcement action should be taken against ASPSPs that are not meeting their obligations under PSRs. This will help to build trust and confidence in UK open banking and deliver a satisfactory service to end-users.

**Question 5: To what extent do you consider the government's objective to facilitate competition by permitting open access to participants or potential participants on reasonable commercial terms has been met?**

We welcome the PSR's Directions in relation to access, and in particular Specific Direction 1 (SD1) on indirect Access to payment systems. It is reassuring for such explicit requirements be set out to which indirect access providers can refer. We welcome in particular the extension of SD1 to all indirect access providers offering sponsor bank services.

We very much welcome the opening of access to settlement accounts at the Bank of England to non-banks.

**Question 6: Are there further barriers preventing open access to participants or potential participants on reasonable commercial terms?**

*Access to bank accounts*

The EMA continues to witness a very low number of Credit Institutions willing to offer bank accounts to the EMI and PI sector, and ongoing issues with de-risking. EMA members' businesses require access to bank accounts, and indeed they cannot function if deprived of access or if this is made difficult.

Article 36 of PSD2 obliges national competent authorities to ensure payment service providers obtain access to bank accounts with credit institutions (CIs). In addition to non-discrimination, objectivity, proportionality and a duly motivated decision by the CI, member states are now required to ensure access is achieved as an outcome.

The time spent and the associated cost to secure and switch to new bank accounts is considerable: CFOs, Finance and Compliance departments and banking relationship teams have to invest a significant amount of time constantly secure new banking relationships. Once the new account has been sourced, the cost/time required for onboarding, integration and implementation can be significant, depending on the service provided (for example offering indirect access to payment systems). These teams would otherwise be in a position to advance products and processes to improve the services offered to customers.

PSPs negotiate commercial terms when they enter into business relationships with other financial institutions: when a business relationship is withdrawn, PSPs are under time pressure to secure a new contract to avoid any disruptions for customers. In addition, the number of Financial institutions offering the currencies, links into payment systems and level of automation needed is limited and PSPs have to therefore often accept more costly arrangements.

To mitigate the risk of being “de-banked” and no longer being able to meet regulatory obligations such as to safeguard client funds and to service customers, PSPs engage with a variety of banking partners. With an ever-diminishing number of banks willing to onboard PSPs, and an increase in the number of PSPs seeking banking services, the cost has increased, and spreading the risk across multiple banks becomes almost impossible, especially for smaller market participants.

Some firms have had to consider closing the e-money segment of their business due to difficulties obtaining an account.

PSPs have to resort to using accounts offered by other PSPs instead of using bank accounts. PSPs’ preference (for business continuity reasons as well as other risk management purposes) is to have several bank accounts in use, but this is often not possible, and increasingly difficult to achieve. Securing banking relationships and keeping those business relationships are vital for PSPs to continue to operate.

#### *Direct Access:*

Connectivity options to FPS currently attract significant setup and on-going operational costs for participants who are required to establish a direct physical connection to the FPS CIP or route via an intermediary. In addition, currently the FPS CIP requires that participants access, and pay for, transaction data as an ancillary service to core transaction processing, via a separate technical connection. Transactional data is a fundamental part of performing payment reconciliations and all FPS participants are therefore compelled to use this extra service at additional costs.

For a small PSP, the upfront technology investment, required knowhow and ongoing maintenance cost for direct participation in BACS is significant. In addition, only a limited number of well-established technology providers exist in the market. This limits the choice

of technology solutions, creates a barrier to entry, and makes scheme access for non-bank PSPs less viable.

*Indirect participation:*

The creation of Directly Connected Non-Settling Participants (DCNSPs) in Faster Payments has been an important step to grant non-bank PSPs better access to the scheme. There are however currently only a limited number of banks offering this model. We would like to see an increased uptake amongst direct participants to give PSPs more options and increase competition.

In relation to BACS, while it technically is possible to establish a direct channel into Vocalink, as yet there is no formal indirect model managed by the scheme. In addition, some sponsor banks have limited experience of assessing the credit risk associated with a PSP for BACS Direct Debit, resulting in excess funding requirements or credit restrictions. This can stifle the ability of Fintechs to start and scale.

*Inconsistent rules and requirements around capital requirements and safeguarding of customer funds*

One of the key areas of focus for governments and regulators in relation to non-bank PSPs is capital requirements and safeguarding of customer funds. There has been a significant increase in international regulation and guidance in these areas for non-bank participants, resulting in an ever increasing burden for companies starting out or looking to scale internationally. For example, the FCA's approach to safeguarding requires 'double safeguarding' in a number of scenarios - both when facilitating transactions via other non-bank providers, but also when considered in the context of international regulation.

**Question7: What do you think industry, regulators and government should do in order to remove these barriers?**

*Access to bank accounts:*

Banks have been given the role of "policing" the non-bank sector for breaches of AML and sanctions rules, and as they are keen to maintain their access to US clearing, they feel compelled to minimise their exposure to any type of AML risk, even if potential rather than real. If the objective sought by HMT is for banks to perform some form of compliance assessment of regulated institutions, this should be set out clearly in Guidance, describing a perimeter for the assessment, the areas in scope and reasonable expectations in this context. Failing to do so will simply give an advantage to bigger and more established businesses, and will provide a means for banks to act in an intrusive and possibly anti-competitive manner.

PSD2 Article 36 offers a unique opportunity to monitor and track the extent of the problem of de-risking, as it allows for the collection of data in relation to declined bank accounts, and - if published - could assist industry in tracking the extent of the problem. HMT should require the publication of data that informs the industry and other public institutions on the percentage of applications that are refused, the basis for such refusals across the industry, and it should

comment on the reasonableness of such refusals. Publication of such granular detail would also assist PSPs in identifying groups or individual CIs that are engaging with PSPs and offering banking services, thus saving resources on the side of both applicant and CI.

The government should conduct a regular review of the data, and assessment of:

- (i) The PSD2 objective of extensive service offerings,
- (ii) The PSD2 objective of obtaining 'unhindered and efficient' service to non- bank PSPs.
- (iii) whether the overall outcome hinders competition or creates a distorted playing field in the provision of payment services

If there is found to be a failure in achieving competition, or the specific objectives of PSD2 provisions are not met, then government should consider intervention and a number of measures introduced elsewhere in the EU may be helpful in this regard:

- (i) The regulator could, in the event of refusal of banking services for a regulated firm, nominate a credit institution to offer such services; a model that has been implemented for all users in France;
- (ii) The Bank of England could consider opening accounts for such institutions at the Bank, enabling a minimum level of service to be offered; a model that is effective in Lithuania
- (iii) Finally, the regulator could take a view on specific refusals and compel the relevant institution to open an account, if it felt that the refusal was unreasonable.

We believe that there is already good basis for intervention, and that the ability of PSPs to offer services has been significantly undermined by the withholding of banking services.

#### *Direct Access to other schemes*

Following the example set by Faster Payments, regulators should work with operators of payment systems such as Direct Debit to continue to press for direct access at technical level for participants of different tiers and complexity.

**Question 8: To what extent do you consider the government's objective for UK payment systems that are stable, reliable and efficient has been met?**

No comment.

**Question 9: What do you think industry, regulators and government should do in order to further ensure UK payment systems that are stable, reliable and efficient?**

No comment.

**Question 10: What is the impact of not having comprehensive scheme rules to deal with how participants should collectively act to resolve disputes and assign liability when a Faster Payment goes wrong?**

We recognise that consumer protection measures may serve to encourage use of FP in some scenarios, and it is important that all stakeholders develop appropriate solutions for when fraud or errors occur. However we do not consider, at this stage, that a centralised

FPS rule change to include further dispute-handling and liability rules within the FPS is a fair or proportionate solution.

The role of the payment schemes should be to create a level playing field throughout the payment chain and to enable the development of innovative products that meet a clear market demand. Several payments' industry initiatives already introduce further safeguards for consumers such as Confirmation of Payee and Request to Pay, and future enhancements such as variable repeat payments, being developed as part of the Open Banking standards, will provide secure mandates and payer verification. All of these services can be considered 'overlays' to the FPS, as envisaged by the Payment Strategy Forum, and will provide improved consumer protection using FP.

The existing liability model for credit transfers is set out in PSR 2017: the issuer bears liability for unauthorised transactions, and the PSU bears liability for authorised transactions. The discussion appears to indicate a possible *shift* in liability for *authorised* transactions.

Changing the liability model for credit transfers so that PSPs may have to underwrite all FP transactions would likely make the cost of using FPS prohibitive for new market entrants, and non-bank PSPs, and ultimately any cost increase will likely be passed onto consumers using FP either directly or indirectly. For PSPs who are specialist payment providers, the business impact would be significant, and highly disproportionate in relation to the cost of fraud to these businesses. For instance, there are many FPS use cases where the risk of APP fraud is extremely low or non-existent. The impact therefore of introducing scheme rules that increase the cost of FPS may be more detrimental than the benefit of providing consumer protection for the relevant existing use cases.

We have set out more detail in our response to Q11.

**Question 11: Are additional scheme rules needed to ensure opportunities for person-to-business payments over the system can effectively compete with major card schemes? If so, how could scheme rules achieve this?**

We do not consider that blanket FPS rule changes, nor simple replication of the rules of the card schemes, are necessary in order for FP to provide a compelling alternative to card payments. Pay.UK's recent consumer research indicates that most consumers use FP as a replacement for cash, and would seek protection only for higher value transfers to new merchants, when they aren't paying for a physical goods and services. This highlights the fact that there are many opportunities for using FP for person to business payments where consumers may not seek additional protections as standard. Adjusting FPS rules based on limited market demand would therefore seem disproportionate.

We also understand HMT's question to be: what would be the impact of introducing rules and functionality into the FPS scheme that enable a **liability shift** to PSPs to bear the risk of non-payment and fraud when it has been authorised by the payer.

When considering the merits of such a shift, it is important to review the purpose of FPS and its many use cases. A payment is a simple transfer of value between accounts. This does not necessarily make it suitable for all transactions. FPS is a low-cost basic payment service that provides the backbone for innovative firms to build upon and offer better

products to customers. This is where FPS holds an advantage over card schemes, and it is a valuable asset to the UK payments systems.

*The rationale for a shift in liability for FPS transactions*

The consultation paper refers mainly to the increase in APP fraud in its justification for introducing a shift in liability to the FPS scheme rules. However in contrast with the majority of fraud experienced within the card schemes, in the case of APP scams, the fraud takes place entirely outside of the domain of the PSP, and the PSP does not have any statutory investigative powers nor the know-how or resources to discover the nature or merits of the claim. This is entirely a matter for law enforcement and for government led action.

APP Scams relate to fraud in the community at large, and not solely to failures in the payment system. Shifting liability for APP fraud to PSPs runs the risk that PSPs will in effect provide an underwriting service for APP Scam fraud, and may end up offering compensation even if no fault can be shown. For example, a failure in the security of an accountancy firm that allows hackers to substitute fake payment details, or poor oversight by a dating web site that allows scammers to perpetrate widespread 'romance fraud' etc. would be regarded as shortcomings to be attributed to the PSP even if the PSP has invested in detecting, preventing and responding to such risks.

This is inappropriate for a number of reasons: (i) it is contrary to the expectations of natural justice where compensation would be expected to flow from fault (ii) it creates a disincentive for third party actors who have the ability to reduce such risk – such as the accountants and dating web site providers in the above examples, to act to reduce the risk; (iii) it encourages fraud by providing victims with compensation in almost all circumstances, and (iv) it leaves the underlying fraud problem, a law enforcement and government policy matter, unaddressed. We note that chargeback fraud, where the customer fraudulently requests a return or refund in the form of a chargeback, accounts for over 30% of card fraud losses, more than the value of losses due to ID theft.

*Impact on EMA members and their customers:*

We note that the examples given in HMT's consultation paper: card schemes, Direct Debit and PayPal, all charge high fees for the consumer protections provided. In addition, we note they have designed proprietary systems to provide those protections with an economic model that is sustainable.

A liability shift affecting all FPS payment use cases would likely result in a change in the cost of Faster Payments for end users as PSPs seek to recover the cost of compliance and credit guarantee, possibly limiting the demand to migrate to FPS from other payment types. In addition, the Confirmation of Payee (CoP) and Request to Pay (RtP) functionality currently being rolled out by Pay.UK would likely need to be mandated in order to support new scheme rules on liability. The potential impact on overlay services such as PIS services could be significant, and make them unviable from an economic point of view.

Increasing the cost of FPS payments is anti-competitive because it favours incumbent institutions with a large customer base. This is because a larger proportion of their customers' payments will be routed within the bank's own payment network and therefore will not be using FPS. For example, for a bank that has a current account market share of 25%, there is a 1 in 4 chance that a payment made by one of its customers will not be an

FPS transfer (because it could be an internal network transfer to another account held at that institution). There is also a growing trend amongst larger banks to set up proprietary payment/settlement systems to net and settle transactions between them, thus avoiding the use of FP.

The income derived by EMA member institutions is usually restricted to that from the payment service itself, and will be limited in scope. It may be a fixed amount that is not related to the transaction size, or it may be a percentage, usually significantly less than 1% of the value of the transaction. In contrast, retail banks have other sources of income, such as credit cards, mortgages and other types of lending that generate considerably more income that is available to subsidise transaction fees. These PSPs will therefore be less able to absorb increases in the cost of FPS, as they have limited or no other sources of income to subsidise such an expense.

Specialist PSPs will be forced to pass the increased cost to their customers, whilst retail banks will be able to subsidise such payments, creating adverse competition conditions that favour incumbents. This will erode competition and increase barriers to entry and take-up of FPS as a service. It is not acceptable therefore that these costs should be foisted on specialist PSPs, resulting in their products becoming less competitive, when in fact their entire business is predicated on creating more efficient and cheaper products than incumbent PSPs and banks.

HMT should make a fundamental assessment of whether a migration from card payments to FP in all use cases is a desired outcome, and therefore whether or not it should be a driving factor in changing the FPS. It is better to achieve a significant but incomplete protective environment for users than to seek an overly ambitious arrangement that has significant unintended consequences on the wider payments ecosystem.

#### *APP scams CRM Code; mandatory application*

EMA members acknowledge the customer detriment that is being addressed by, and certainly support the aims of, the APP Scams CRM Code. However, many EMA member firms have not joined because the requirements of the Code place a disproportionate compliance burden compared to the (current) risk posed to EMA members and their customers.

Whilst EMA members support the use of tools such as Confirmation of Payee, transaction monitoring, freezing of queried funds and ongoing customer education, there are many additional requirements the Code imposes that are not proportionate to their APP-scam volume, which is a fraction of that experienced by the existing signatories of the Code.

This is understandable, as the Code was designed to mitigate a risk to which banks - where customers tend to hold their main deposit accounts – are much more exposed. The EMA would therefore strongly resist the mandating of the Code for non banks for the primary reason that the cost of compliance is hugely disproportionate to the APP scam risk observed in this sector.

Mandating the adoption of the Code for all PSPs in the UK, via FPS scheme rules or another mechanism, regardless of risk or exposure to APP scams, or of business model, would create a barrier to entry for smaller or new PSPs wishing to enter the market. Instead a risk-

based approach should be adopted, taking into account firms' business models and exposure to APP fraud in order to ensure consumers are appropriately protected.

*Proposed solution: access to payment schemes*

If the government's goal is to promote competition, and in particular competition against the card schemes, a more effective tool would be to address the issues with access and payment scheme infrastructure, which could germinate all kinds of competition. The New Payments Architecture will be able to provide that level of access, and the first overlay services have already been developed: Confirmation of Payee and Request to Pay.

**Question 12: Why are payments with a longer clearing cycle still used and what are the barriers to moving these payments to a platform with faster clearing, e.g. Faster Payments?**

We recognise there may be cases where longer clearing cycles may be beneficial. However, we note that often when PSPs opt to use BACS, rather than FPS, the extended clearing time may only be one of the deciding factors alongside other features of the BACS scheme that meets their particular business requirements.

Instead, clearing and settlement times could be provided by way of a service that is overlaid on top of the clearing/settlement platform – as is envisaged for the NPA – rather than being a core feature of the payment scheme itself. An overlay service would allow greater flexibility and innovation, ultimately benefiting consumers, businesses and merchants.

**Question 13: What is required to enable Payments Initiation Services to take off in the UK in a way which is safe and secure for the consumer?**

We have set out our views under Q4. We do not consider that not having a consumer protection regime as part of FP is the main reason that PIS payments have not "taken off". We do recognise that consumer protection is an important factor when considering whether PIS can effectively compete with card payments in a retail environment, but note that PIS have been able to grow in other markets such as the Netherlands or Sweden without the need for a chargeback regime that mirrors card schemes. As discussed in Q10/11, we believe that changing the liability model for FP without sufficient analysis of the impact to the payments market may, in fact, hinder the growth of the PIS market in some sectors, which is still in its infancy.

Instead, at this early stage of open banking's evolution, we consider that the immediate priority is for HMT to assist with driving forward a robust, fit-for-purpose ecosystem so that third-party providers (TPPs) can rely on API interfaces provided by ASPSPs to deliver products and services. In turn, this will enable consumers and businesses to build up confidence in those services in substantial numbers and realise the benefits of open banking.

The continuation and completion of several items in the Final Approved Open Banking Roadmap is key to facilitating the growth of a dynamic, large scale intermediary sector (AIS, and PIS providers, and technical service providers). This is particularly important for the

Roadmap items that relate to developing payments functionality, so as to support PIS providers bringing viable propositions to market.

We have summarised below a number of key issues where HMT could take action to ensure that viable payment initiation services can develop in the UK market.

As discussed in full in our response to Q4, we believe HMT could take targeted action at both a legislative and oversight level to ensure that viable payment initiation services can develop in the UK market.

**Regulatory Framework:** a review the PSRs and the UK-RTS to fully realise the benefits of open banking including: clarify the definition of AIS, the regulatory perimeter for PIS, and address barriers to providing compelling PIS propositions in the UK-RTS, would create a solid platform for commercially-viable PIS products which meet clear consumer demands.

**API performance and implementation:** address the issues of open banking API availability and performance to ensure that a ‘two-tier’ API ecosystem does not evolve where open banking API performance and operational resilience are sub-optimal in comparison to ASPSPs commercial API services. The poor performance of ASPSPs’ open banking API infrastructures for TPPs can already be seen to be providing ASPSPs with an advantage when they decide to provide AIS/PIS services.

**Open Banking Future Governance:** the future governance model for Open Banking should be resolved as a matter of urgency so as to provide a degree of certainty to the ecosystem, and provide the basis for longer term planning and investment in PIS products.

**Question 14: How does the advent of Payment Initiation Services through Open Banking interact with your answer as to whether additional rules are needed as part of Faster Payments?**

Additional FPS rules and liability regime could increase the cost of the FPS and introduce a downstream impact on PISPs’ ability to provide viable PIS/Open Banking product/services. It may also encourage a migration away from Faster Payments towards proprietary closed systems which would act as a further disincentive to develop PIS propositions based on FP.

**Question 15: Will Open Banking deliver (and go beyond) the developments in account-to-account payments seen internationally? What are the lessons from international experiences that should be adopted in the UK, and what are the costs and benefits of doing so?**

International developments in account to account payments can lead to a few observations on applicability to the UK market:

- **Payer preference in a given country should not be discounted.** Account to account payments schemes have gained acceptance in countries where credit is not popular (Netherlands, Germany etc). In the UK, card payments are preferred by consumers and merchants in many use cases. The reason for switching from card to account to account transactions would have to be compelling for payers to facilitate a change in behaviour.

- **Evolution of the UK's payment ecosystem will take time.** iDEAL in the Netherlands started slowly, but has grown to become the preferred e-commerce payment option over the past 10-15 years. HMT should encourage the growth of PIS and Open Banking but consider that it may take time to gain traction and not to further intervene before all market participants have had the opportunity to realise the return on investment.
- **Regulation as an enabler, not a driver.** Banks and PSPs must be sufficiently commercially incentivised to provide compelling account to account payment services. This will only be achieved where the services developed are driven from clear customer and market demand as in the case of iDEAL, Swish, Sofort, and other international initiatives.
- **Customer journey is key.** Convenient and user-friendly customer journeys will play a critical role in driving the adoption of account to account payments. The UK Open Banking standards have undoubtedly driven the UK's leading approach for PIS, but there are number of issues with regards to the scope of payment services supported, and the user's payment journey for PIS (see our responses to Q4 & 10) which will need to be addressed to reduce payer friction.

**Question 16: Do you agree with the trends in new service providers and payments chains identified?**

The break up of the payment value chain has been a feature of payment services for some time. The increasing complexity of payments, and the smaller profit margins has meant that specialist service providers such as card processors or cloud storage providers or indeed compliance service providers are often required to be able to deliver competitive solutions.

The diversity of entities that choose to become regulated as EMLs or PIs, often to maintain control over their consumer solution, has meant that the use of third party service providers for acquiring technical services, or for cross border payment functionality or for support services such as customer support or CDD has become more widespread. This does complicate the supervisory and oversight functions, but also introduces specialisations that could provide reliable and consistent service levels that are predictable and effective parts of a regulated payment service.

We believe the increasing complexity of products as well regulatory expectations are likely to result in a greater need for specialist service providers addressing the different parts of the payments value chain.

**Question 17: What further trends do you expect to see in payments chains in the next 10 years?**

The increasing sophistication of users, the increasing penetration of technology into business and daily life will result in the embedding of payment functionality into a range of business and human interactions. Payments could be contingent on certain conditions being met (so called smart contracts), they could be authorised verbally through personal assistants, or they could be inherent in the context of transactions, such as riding a cab, or walking out of a supermarket.

These developments will depend on the availability of APIs that will enable third party services to authorise or initiate payments, or the availability of payment products that enable cross border payments with the same ease as local or national payments.

The continuing development of distributed payment products will inevitably lead to niche or broad implementations that will offer unique benefits to users and consequently to more widespread take-up by users. These could be based on a range of crypto assets with very different attributes.

The increasing pace of development of central bank issued digital currencies (CBDC) also poses a broad set of challenges to payment products that are based on bank money or on e-money. The CBDC model that is adopted could create a competitive challenge for existing PSPs, or may offer a new product and a level playing field for private PSPs.

**Question 18: What opportunities and/or risks do these trends in new service providers and payments chains pose?**

Please see our response to Q17.

**Question 19: What do you think industry, regulators and government should do in order to realise these opportunities and/or address these risks?**

*Electronic Money Regulations & safeguarding of funds*

There appears to be a difference in view within industry regarding the status of safeguarding accounts held by e-money institutions (EMIs) to safeguard the equivalent value of their customers' funds. We would welcome consideration by HMT of clarification that e-money funds are not held on trust by EMIs on behalf of their customers. The concept of a trust is noticeably absent from legal systems in most EU jurisdictions. Given the ability of EMIs to utilise any EEA credit institutions to hold such funds, it would seem reasonable to suggest that this was not contemplated by the European legislator when EMD2 was adopted in law.

We note HMT's reference to the fact that e-money funds are not protected by the FSCS. In fact, a very broad range of risks are mitigated under the EMRs safeguarding regime, while they are not addressed or are less specifically addressed under the credit institution regime. We have set this out in further detail below.

Safeguarding involves a number of restrictions that are placed over the assets, including:

- (i) the type of institution where the funds can be deposited,
- (ii) restrictions preventing any use of the funds by the EMI/PI while they are held
- (iii) restrictions on the type of assets that the funds can be held in, chiefly low risk liquid assets
- (iv) restriction on commingling of funds with other funds held by the institution
- (v) restrictions preventing any other party from having any right or interest over the asset
- (vi) Requiring the account to be clearly identified as a safeguarding account

- (vii) Providing, in the event of insolvency, for claims by customers to be met ahead of other creditors.

The restrictions are intended to minimise the risks associated with the holding of the funds by the institutions.

It is worth noting that the restrictions mean that the EMI or PI cannot lend the funds to a third party, as for example banks do with deposits, cannot invest in longer term deposits or higher risk investments, and cannot use the funds as collateral or security in relation to any financial activity.

### *Analysis of risks*

The safeguarding risks associated with electronic money institutions relate to an ongoing commitment to redeem outstanding e-money that is held by users with the EMI, while that for payment institutions relates to settlement risk, as PIs do not hold funds for users on an ongoing basis. This difference is reflected in the differing initial and ongoing capital requirements associated with the different types of institution.

Operational risks are however similar, and these are mostly mitigated by the restrictions placed on the account; see items (i) to (vii) set out in section 1 above, or require additional mitigating measures to be put in place.

The risks that remain to be addressed by the firms through other mitigating measures are chiefly, those of market failure, compliance, and financial crime.

- (i) In the event of the credit institutions holding the funds failing, then the safeguarded funds will be vulnerable, and may be lost in part or in whole. In order to address market risk, the advice is to assess the soundness of the institutions that are chosen to hold the funds, and to do so on a periodic basis.
- (ii) Compliance failures may result from the firm failing to safeguard sufficient funds, or in using the funds for operational expenses, or failing to recognise the nature of the funds and allowing third party access or a security to be applied.
- (iii) Financial crime can take a variety of forms, from insider fraud to cyber crime that may comprise an attack on the business or its banking partners.

Whilst not exhaustive, the above risks can to a large extent be managed, mitigated, and be made subject to corresponding compliance controls.

This can be supported with appropriate supervisory oversight that could seek to identify poor practice, potential failure and ensure it is remedied.

The FSCS acts as a safety net of last resort, and by definition can only address a limited degree of harm; it cannot compensate for all funds that could be lost in the event of the failure of an institution or multiple institutions, and hence a maximum claim limit is set per individual claimant.

The FSCS is not in our view, a supervisory tool or a means of mitigating risk, such as those risks relating to the safeguarding of funds. It provides some modicum of compensation to depositors and other claimants in the event of failure.

It remains therefore to consider whether the FSCS is an appropriate tool for dealing with failure in the electronic money and payment institution sector.

We have set out below a table comparing the risks associated with the holding of payment service related funds for EMIs and PIs with those for credit institutions undertaking the same business. The table below demonstrates that a broad range of risks are mitigated under the safeguarding regime, while they are not addressed or are less specifically addressed under the credit institution regime.

**Table providing an overview of the risks that attach to payment service- related funds when held by EMI/PIs and when held by credit institutions.**

Risk to funds held for payment service users	Application to EMI/PI	Application to a credit institution	Comments
Investment risk, - loss in value of funds	Low risk assets	Only requirement is to hold appropriate capital; can also lend	
Liquidity risk –non availability for redemption	Funds are always available	Funds subject to overall liquidity requirements	
Diminution due to use of funds for operational purposes	This is not permitted	Only requirement is to hold appropriate capital	
Diminution due to access by third parties	This is not permitted	There is no restriction	
Risk arising from third party interest over the funds	This is not permitted	There is no restriction	
Risk of set-off by the bank or custodian	This is excluded contractually	This is present	
Risk of claims by other creditors in the event of insolvency	Users are given preference by statute	Users sit as equals with other creditors	Note FSCS may be available – see final row below
Risk of compliance failure, resulting in diminution or erosion of funds	This can take place	This can take place	This has been the basis of a number of enforcement cases against PIs, usually cash based money remitters
Risk of internal fraud	This can take place	This can take place	

Risk of external fraud, such as a cyberattack resulting in losses to safeguarded funds.	This can take place	This can take place	This could for example
Ultimate risk of non payment to users.	This is possible where the fund is diminished	This is possible for e- money products that are not covered by the FSCS; and then for other payments only above losses of £85,000 per person	

**Question 20: Do you think any changes are needed to payments regulation to ensure it keeps pace with the changing technological landscape?**

Please see our responses to Q4 in relation to Open Banking.

**Question 21: What further trends do you expect to see in cross-border payments in the next 10 years?**

No comment.

**Question 22: What do you think industry, regulators and government should do in order to improve the functioning, speed and cost of crossborder payments for consumers taking into account the G20 work?**

The EMA supports any efforts to improve direct accessibility to payment systems for new participants as a global standard: improving competition and having simpler onboarding processes will allow a wider range of businesses to have access, and can only benefit and advance payment service users.

We are supportive of price transparency, and believe that this is likely to increase competition as consumers become better aware of the total cost of an exchange transaction. It is also likely to increase consumer value and consequently have a positive wider impact in the market. It is important that consumers can make informed judgements on the relative value offered by third party currency conversion service providers, in comparison with the alternative bank or card scheme conversion offered to the user as part of their payment product. There is for example little indication of the value of the variable fee embedded in the exchange rate, and the total cost of the transaction is seldom disclosed to the consumer.

**Question 23: Are there other opportunities and risks not captured by the questions elsewhere that you wish to highlight? If so, what do you believe the role is for government, regulators, and industry in responding to them?**

No comment.



**List of EMA members as of October 2020:**

[AAVE LIMITED](#)  
[Account Technologies](#)  
[Airbnb Inc](#)  
[Airwallex \(UK\) Limited](#)  
[Allegro Group](#)  
[American Express](#)  
[Azimo Limited](#)  
[Bitstamp](#)  
[BlaBla Connect UK Ltd](#)  
[Blackhawk Network Ltd](#)  
[Boku Inc](#)  
[CashFlows](#)  
[Ceevo](#)  
[Circle](#)  
[Citadel Commerce UK Ltd](#)  
[Coinbase](#)  
[Contis](#)  
[Corner Banca SA](#)  
[Crypto.com](#)  
[Curve](#)  
[eBay Sarl](#)  
[ECOMMPAY Limited](#)  
[Em@ney Plc](#)  
[ePayments Systems Limited](#)  
[Euronet Worldwide Inc](#)  
[Facebook Payments International Ltd](#)  
[First Rate Exchange Services](#)  
[FIS](#)  
[Flex-e-card](#)  
[Flywire](#)  
[Gemini](#)  
[Globepay Limited](#)  
[GoCardless Ltd](#)  
[Google Payment Ltd](#)  
[IDT Financial Services Limited](#)  
[Imagor SA](#)  
[Ixaris Systems Ltd](#)  
[Modulr FS Europe Limited](#)  
[Moneyhub Financial Technology Ltd](#)  
[MuchBetter](#)  
[myPOS Europe Limited](#)  
[Nvayo Limited](#)  
[OFX](#)  
[OKTO](#)  
[One Money Mail Ltd](#)  
[OpenPayd](#)  
[Optal](#)  
[Own.Solutions](#)  
[Park Card Services Limited](#)  
[Paydoo Payments UAB](#)  
[Paymentsense](#)  
[Payoneer](#)  
[PayPal Europe Ltd](#)  
[Paysafe Group](#)  
[Plaid](#)  
[PPRO Financial Ltd](#)  
[PPS](#)  
[Remitly](#)  
[Revolut](#)  
[SafeCharge UK Limited](#)  
[Securiclick Limited](#)  
[Skrill Limited](#)  
[Soldo Financial Services Ireland DAC](#)  
[Stripe](#)  
[SumUp Limited](#)  
[Syspay Ltd](#)  
[Token.io](#)  
[Transact Payments Limited](#)  
[TransferMate Global Payments](#)  
[TransferWise Ltd](#)  
[TrueLayer Limited](#)  
[Trustly Group AB](#)  
[Uber BV](#)  
[Vitesse PSP Ltd](#)  
[Viva Payments SA](#)  
[WEX Europe UK Limited](#)  
[Wirecard AG](#)  
[Wirex Limited](#)  
[WorldFirst](#)  
[WorldRemit](#)