UK FINANCE

Payment Services Regulations – Call for Evidence

UK Finance response

6 April 2023 v4.0

Executive Summary 2

Response to questions 4

General questions 4

Scope and definitions 6

The regulatory treatment of payment services and e-money 8

Information requirements for payment services 9

Rights and obligations in relation to the provision of payment services 13

Wider considerations in relation to the provision of payment services 15

Fraud 16

Strong Customer Authentication 17

Issuance and redeemability of electronic money 19

Miscellaneous 20

Appendix A: Specific changes relating to Strong Customer Authentication 22

Appendix B: Consent for use of personal data 23

Appendix C: Stable Coin: Separate paper

Executive Summary

- The UK is home to one of the most advanced and dynamic payments sectors in the world. UK Finance welcomes this review and Call for Evidence as an opportunity to work towards a proportionate approach to regulation that is based on principles and outcomes, driving even more growth and innovation for the UK payments sector. We support the approach provided for by the Financial Services and Markets Bill (FSMB) to delegate additional powers to the regulators involved in payments – Bank of England, FCA and PSR – to allow for a more flexible and nimble approach to regulating what is a rapidly evolving market.
- As a result of retained EU law, many different levels of law and regulation exist in the UK, for example, the PSRs themselves, the FCA handbook, FCA approach document, RTSs, and increasingly new FCA guidance being published via 'Dear CEO' letters or similar. We would welcome consolidation, simplification and an orderly reduction on these levels of regulations.
- We believe there are opportunities to be grasped in making the domestic regulatory framework for payments more outcomes-based. This will allow market participants to compete and innovate in a way that delivers the desired outcomes for customers. A good example is gradually removing some of the prescription in Strong Customer Authentication requirements which are technology-specific, while ensuring that payment service providers (PSPs) continue to monitor and improve on security of payments.
- UK Finance would like to underline two major requirements as part of any change to the domestic regulatory framework for payments.

Regulatory coordination, accountability and certainty

- A payments sector served and represented by a dynamic and varied body of firms, which has and continues to meet the cost and demands of significant regulatory change, requires a regulatory framework with certainty and proportionality at its core. Such a framework can be enhanced by greater coordination of policy initiatives by government and the relevant regulators, both in terms of content and in terms of implementation requirements and timelines. Regulation and supervision must deliver certainty to market participants so that products can be developed and investments made in firms. The Regulatory Initiatives Grid is helpful but only if it helps reduce the regulatory burden; for example, currently there are multiple regulatory consultations that need to be considered holistically as they are interrelated and to avoid unintended consequences. The consultations include, but are not limited to PSRs, BNPL, CCA reform, OB/JROC, safeguarding and insolvency, ECB, APP fraud, CoP, CBDC and crypto.
- As we have argued previously,1 for regulators to effectively advance their statutory objectives at minimum cost and risk of unintended consequences, it is vital that their interventions be made on a sound evidential footing. To that end, we strongly welcome the measures in the FSMB to strengthen the requirements governing how the regulators conduct cost benefit analyses (CBAs) and review existing rules. Transparency in policymaking is essential to giving firms confidence that regulators have properly considered all relevant matters. Seeing this analysis would also give the industry an opportunity to identify potentially missing data or evidence. It is also crucial that there be sufficient and proper consultation on new rules or substantive rule changes by the regulators.
- Regulators, like all public bodies, should be accountable under the law for meeting their statutory duties. This is the key regard in which the Future Regulatory Framework measures implemented by the FSMB fall short, with the result that the regulators' enhanced roles will not be matched by enhanced accountability, to the detriment of the overall regulatory framework. This is the subject of live debate in the final stages of Parliament's scrutiny of the FSMB, and we are committed to working with the government to ensure the right mechanisms are in place, including on the role played by Parliament in scrutinising the regulators. We have previously recommended the establishment of a

---

[1] UK Finance response to the Financial Services Future Regulatory Framework Review
https://www.ukfinance.org.uk/system/files/UK%20Finance%20response%20to%20FRF%20consultation%20on%20proposals%20for%20reform.pdf

new rule review mechanism – open to those affected by regulation – based on the existing super-complaint model, and continue to believe this would be a viable solution.

EU and international access

- With UK payments firms operating internationally, this can benefit customers by creating new competition and choice when they consider which solutions they wish to use. As the UK adapts its financial services rules and regulations post-Brexit, we welcome the UK's approach of tailoring its financial services regime to the UK's unique characteristics. This means that, where the UK decides to diverge from EU rules, it is not done so for divergence's sake. This is particularly important for the UK given it is a leading international financial centre, where many firms operate in other, jurisdictions including the EU (in which maintaining market access to the euro payments space is a key priority for our members).
- Ongoing access to SEPA remains of strategic importance for the UK payments industry. It is therefore important that EU/EEA legislative provisions which underpin the UK's access to SEPA continue to be applicable in the UK. This can, for instance, be through UK legislation, or in equally binding practice (in accordance with the SEPA Participation Criteria). This includes legislation such as PSD2 and the SEPA Regulation, which is necessary for the UK to retain its membership of SEPA, and for its PSPs and their users to be able to continue to send and receive SEPA payments. HMT and regulators should publicly consult on all legislation, rules and guidance that are intended to revoke and replace retained EU law, even if this is believed to be simply a restatement of existing legislation.
- In line with the government's objective to 'facilitate the international competitiveness of the UK economy', regulators should also have regard to the G20 Roadmap on enhancing cross-border payments. This is because global standards can provide a common set of aims which, in turn, can help to align the intent and approach of domestic regulations across markets, even if they differ in detail. The priorities for the next phase of work on the G20 Roadmap focus on (1) payment system interoperability and extension; (2) legal, regulatory and supervisory frameworks; and (3) cross-border data exchange and message standards - all of which point to a need to be mindful of global developments.
- **In this response we cover** detailed comments on the following topics:
    - Implications of merging the PSRs and EMRs, and bringing new firms within the payments perimeter.
    - A risk-based approach to help prevent fraud (including allowing PSPs to pause the processing of a Faster Payments transaction in cases where they reasonably believe there is a heighted risk of fraud).
    - Removing some prescription from Strong Customer Authentication to improve customer journeys while retaining the overall objective to reduce fraud in electronic payments.
    - Opportunities to improve customer information.
    - Safeguarding arrangements.
- **In this response we do not cover** detailed feedback on open banking, including on the relevant questions within the Call for Evidence. This is because UK Finance is awaiting the outcome of the JROC deliberations and needs to digest this information before it can give detailed feedback on the regulatory framework for open banking.

Response to questions

General questions

1. **How should the payment services framework evolve – and what should be the government's priorities – to better promote the following government objectives for payments regulation:**

   A. Achieving agile and proportionate regulation, which facilitates the international competitiveness of the UK economy through growth and innovation in the UK payments sector.

   B. Ensuring appropriate trust and protection for consumers.

   C. Ensuring the resilience and integrity of the UK's payment market.

   D. Fostering competition, in the interests of consumers.

   UK Finance agrees that these are key objectives for the regulatory framework. We believe that the following principles will help regulators meet and refine these objectives.

   Outcome-based and market driven approaches, shifting away from prescriptive regulation

- Overly prescriptive regulations impede competition and are particularly onerous for challenger firms. UK Finance advocates a regulatory framework that is outcomes-based, allowing firms to compete and provide innovative products for all different types of customers.
- We believe that simplification of the UK regulatory landscape would help meet this principle, introducing more flexibility and encouraging further innovation and investment. The current regulatory framework is difficult to navigate with a multitude of regulations, rules and applicable guidance that sit beneath or alongside the PSRs. Certain parts of the PSRs (such as the Schedule 4 Information Requirements) and associated Regulatory Technical Standards (the RTSs) can take an overly prescriptive approach and would benefit from being reviewed and subsumed into rules or guidance. For example, this would grant the FCA the opportunity to designate certain parts of the RTSs as rules or guidance - enabling a more agile supervisory approach which would be desirable in areas such as Strong Customer Authentication (SCA).
- This should however be balanced with the need to ensure regulatory certainty for PSPs and that regulator scope creep is minimised. Firms should be provided with clarity on minimum requirements to achieve compliance.

Consider outcomes for all end users, including consumers, merchants and corporates

- It is important to recognise that payment providers serve a range of end-users and to avoid a one-size-fits-all approach. Payment service users (PSUs) encompass consumers (including vulnerable and high net worth individuals); businesses (small and large); government (central and devolved); and other PSPs or financial institutions (including indirect participants accessing infrastructure through a variety of mechanisms). These end users have different needs, including on access and service levels; and they also have different commercial, bargaining and technology positions. It is essential, therefore, that there continues to be meaningful consultation with industry and stakeholders on any changes to the regulatory framework so that all of these needs can be taken into account. The example, consideration on the disapplication of provisions (e.g. corporate opt-out, SCA and the secure corporate payment exemption) in specific circumstances.
- For example, as new payment propositions expand, regulators have a role to play in ensuring some level of consistency in protections against purchase risk and fraud. PSUs should know how they are protected and understand who to turn to in the event of a question or complaint about a payment. This is an important enabler of the trust that consumers and businesses have in the payments that they make. However, it is vital not to take a one-size-fits-all approach when the needs among PSUs diverge so greatly.

Same activity, same risk, same regulation, applied proportionately

- Without this principle being applied, firms can face the same scrutiny at the point of authorisation and incur significant cost of regulation despite posing different levels of risk; or firms can undertake the same activity but face different levels of conduct regulation. For regulators to have effective oversight of activities in payments, they should consider recalibrating the mix of entity-based and activity-based rules.
- Because the same activity can generate different risks depending on who performs it (i.e. systemically important firms versus smaller firms), regulatory asymmetry is to be expected. A current example that regulators are looking to accommodate is the growing presence of Buy-Now-Pay-Later (BNPL) products in the market. BNPL products blend traditional credit elements with payment elements, and are being offered by a range of entities, demonstrating the need for a dynamic regulatory regime.
- Regulators must ensure that scope creep is minimised and significant changes to regulatory environments go through due process. For example, on BNPL, it is important that the credit and payment elements are addressed through the appropriate legislative framework (indeed the recent HMT consultation addresses the credit-related elements separately from the payment-related aspects). Regulators should ensure that the benefits of these adjustments can be felt by the whole market, enabling new, existing and pioneering firms to develop and deploy innovation effectively within an open and competitive market.

Technology-neutral regulation

- UK policymakers should focus on regulating the application of emergent technologies rather than the technology itself, and enabling their use to achieve defined outcomes rather than enforcing prescriptive solutions. This is not an easy task in payments, where the operation of payment processing is heavily reliant on technology, and where industry standards are often necessary. Regulators should continue to take a balanced approach to engaging with standardisation initiatives and must provide the right incentives and conditions for industry to develop these standards, while avoiding creating technical lock-in and restricting competition and innovation.
- For example, with the adoption of cloud technologies within financial services, ongoing collaboration between regulators and industry is necessary to ensure realisation of the interoperability and scalability benefits.

Creating a level playing field, recognising the need for commercial arrangements

- Payments is a competitive market. Consumer and merchant choice has increased rapidly in recent years, benefitting users by reducing the cost of acquiring and improving efficiencies in payment provision. Consumers now have an increasing number of ways to pay at checkout, including account to account payments, Buy-Now-Pay-Later (BNPL), traditional instalment credit and e-money. In order to maintain this competitive market and the associated benefits for consumers, regulators and legislative bodies should ensure all types of payment methods are given a level playing field to operate from. For example, there should be a view to consistency in regulating financial promotions for different payment types, and also the checkout process itself.[2]
- Payments cost money to provide. This is often something overlooked by regulators, but this oversight further entrenches the difficulty of new service providers to thrive, because in turn it can make services based on interbank payments prohibitively expensive to provide. The cost of doing business and creating new business models in the payments industry is increasing. This is not just the cost of innovating and implementing both mandatory and non-mandatory change, but the operational and investment costs to all providers. This requires the development of sustainable commercial models , including to support customer protections. While particular incentives are required to establish a nascent market, this should be reviewed and rebalanced as markets evolve.

[2] As an example, Strong Customer Authentication is required for credit card transactions but not for BNPL; conversely, financial promotion requirements will apply at the Point-of-Sale (payment button) to the credit aspects of BNPL, but not to the corresponding credit card (payment button).

2. **To what extent would you support rationalising and/or removing the distinctions in regulation between payment institutions and electronic money institutions – in effect, combining the two sets of legislation? Would this be easier for the sector to navigate and/or lead to better outcomes?**

- UK Finance agrees that there would be merit in consolidating the Payment Services Regulations 2017 (PSRs) and Electronic Money Regulations 2011 (EMRs) into one regulation: the EMRs cross refer to the PSRs at numerous points and there is a large degree of repetition in certain sections (by way of example, the same or similar threshold conditions, authorisation process, safeguarding requirements and exclusions apply in both the PSRs and EMRs) which can lead to confusion, particularly for firms trying to navigate and comply with both sets of legislation. Removing this layer of confusion would ultimately lead to better outcomes as firms would be better placed to understand the regulatory obligations applicable to the services they provide. We note this approach would also be aligned with the FCA's "*Payment Services and Electronic Money – Our Approach*" (the **Approach Document**) which covers both regimes.
- The most practical means of implementing this would be to treat the issuing of e-money as an additional permission within the PSRs (albeit noting that the payment services apply in respect of "funds", one of which is e-money), with specific provisions for e-money where there is divergence. For instance, there could be separate chapters for the prudential requirements applicable to each of APIs and EMIs. This could, in turn, encourage competition as firms and new market entrants will have a better understanding of the broader spectrum of services or activities they could provide under the single regulatory regime. This could also enable a firm to progress from being an API to an EMI through a 'variation of permission', i.e. the addition of e-money issuance, rather than through a wholly new authorisation application.
- The revised regulation would also benefit from the merger of certain related secondary legislation, namely the Cross Border Payments Regulation and the Payment Accounts Regulations, noting that the Payment Accounts Regulations are only applicable where the customer is a consumer. Again, this would enhance regulatory clarity and mitigate the current issue of having numerous pieces of disparate regulation that can lead to confusion.[3]
- Any combined legislation must ensure clarity and avoid (a) confusion on what requirements apply to which activity and (b) any unintended consequences – in particular, firms which are not currently in scope of particular requirements (e.g. under the Payment Account Regulations) should not be brought into scope of such requirements as a consequence of the merger. Clearer statements of applicability for firms at the start of each part/section may help. For instance, should the Payment Accounts Regulations be merged into the PSRs, it should be made clear that the corporate opt out would apply. There would also need to be recognition that the definition of 'payment account' under the PSRs is distinct from the definition of 'payment account with basic features' in regulation 19 of the Payment Accounts Regulations. Such an exercise should also not be used to revamp the concept of e-money (without proper consultation).

Scope and definitions

3. **Are (a) the definitions and (b) the scope of the regulated activities in the payments services and e-money framework clear and do they capture the right actors and activities within regulation?**

- In recent years, the UK payments market has become an increasingly diverse and complex industry that continues to evolve rapidly. Fuelled by developments in technology, new market entrants, and a desire for ever-simpler, easier, quicker solutions for users, payments have 'behind the scenes' become much more complex, with a greater number of actors involved, more parties 'touching' the funds or involved in the execution of the payment transaction, and more intermediaries and service providers. This creates certain complexities, which in turn can pose certain problems.

- The UK is one of the most sophisticated, mature, resilient and innovative payments markets in the world, and we want to ensure that changes to the regulatory framework continue to support all of these characteristics. UK Finance members have identified some areas, however, in which existing definitions and scope of regulations could be clarified. We have separately responded to set out in HMT's Payments Regulation and the Systemic Perimeter Consultation, so we have not gone into detail on the specific proposals laid out there.[4]
- Due to the much wider ecosystem, implementing change will naturally take longer. An example of this is the SCA roll-out; where gateways, merchants and indeed users had to be taken on a journey towards compliance. HMT, the FCA and the Payment Systems Regulator need to take this into account when introducing regulatory change: regulated firms have only a certain influence over non-regulated firms and the time for non-regulated firms to change their systems needs to be factored in. This is part of the challenge that PSPs are currently facing in ensuring that the customer outcomes are met in the Consumer Duty, for example.
- Equally, the default position should not be that PSPs are automatically liable for everyone else's actions in the execution of a payment transaction – especially where other firms have customer relationships. Holding them liable too would also create accountability and responsibility to their customers.

Regulation of systemically important service providers

- There are a number of service providers in the payments chain. These underlying service providers are typically not regulated, yet they may nonetheless have customer-facing profiles, often strong ones, which can lead to customer confusion as to the roles being played. An example of this is wallets provided to users on their mobile devices (Apple Pay, Google Pay and Samsung Pay). The customer-facing profiles for such wallet providers (which essentially provide a service to card issuers) puts them in a different place to say, gateways (which provide their services 'behind the scenes' to the underlying merchants).
- The customer-facing nature of such providers builds in additional risks which PSPs cannot manage individually; UK Finance believes that government should consider bringing such firms into the regulatory perimeter in some way. The risks that such critical service providers pose to PSPs include: (a) concentration risk; (b) operational risk; and (c) regulatory risk. There is a need for such firms to recognise they are operating in a regulated environment, and that they are providing a form of outsourcing to PSPs; for example, accepting the application of the EBA Outsourcing Guidelines and/or of their role in 'major incident reporting' to the FCA and PRA.
- We see a similar trend in regulating similar service providers in Europe with DORA5, which will apply from 17 January 2025, and with the ECB's comments recognising that the term 'payment arrangements' is broader than 'payment systems'. We also note that while historically PSD2 has addressed access to payment systems and to bank account services, PSD3 may also be extending these 'access' provisions.
- We note that the Bank of England's proposals for a digital pound could potentially mean that wallet providers (referred to as PIPs: Payment Interface Providers) will be regulated, further confirming this trend towards a greater number of customer-facing roles, and the need for regulation to expand accordingly.

---

[4] https://www.ukfinance.org.uk/system/files/2022-10/UK%20Finance%20Response%20to%20HMT%20Payments%20Regulation%20and%20Systemic%20Perimeter%20v09%20%28002%29.pdf

[5] The Digital Operational Resilience Act (DORA) places specific obligations on service providers that are deemed "critical", a classification that is based on the provider's systemic importance to other financial entities (i.e. through the provision of key ICT services), and the potential risk posed to financial services in the event the service provider faces a large scale operational failure. DORA will place such entities under the supervisory purview of one of the European Supervisory Authorities (ESAs), one of which is the EBA, with several accompanying compliance requirements such as: establishment of a local subsidiary, mandatory operational resilience testing, more thorough reporting and record-keeping obligations and crucially, an oversight fee.

4. **Do the exclusions under the PSRs and the EMRs continue to be appropriate (includes limited network, electronic communication, commercial agent etc)?**

   We believe other industry bodies (such as the Electronic Money Association and Payments Innovation Forum) are better placed to comment on Q4-8. The only observation we would make is that there is an increasing spectrum of firms that are authorised, regulated or registered and it is increasingly difficult to discern between them, both from a customer perspective (in terms of understanding what regulatory protections they may enjoy) and also from a bank account provider perspective (as it requires greater due diligence of firms to fully understand their business model and why they are, or are not caught by the regulatory regime). The latter point goes to both the availability of such bank account services and also to the many other types of businesses which hold funds but subsequently rely upon being out of scope or under an exclusion. Such perimeter issues will always exist, however, they are getting more and more involved, so are affecting banks' assessment of and willingness to provide regulated services.

The regulatory treatment of payment services and e-money

5. **How, if at all, might the framework for the authorisation of payment institutions and electronic money institutions be reformed?**

   In the authorisation of account information service providers (AISPs) and payment initiation service providers (PISPs), there is an ecosystem risk for Open Banking if AISPs are not sufficiently scrutinised and regulated, which needs to be borne in mind when considering any reform to authorisation requirements. Members would wish to see proportionate but sufficiently vigorous provisions in this space to prevent bad actors from entering or incidents, such as data leaks, occurring. UK Finance would need to review the detail of any proposals to change the authorisation framework of AISPs, in order for its members to better understand any potential impact on them.

   Please also see our response to Q3 (in terms of regulatory perimeter) and Q4.

6. **How, if at all, might the framework for the registration of small payment institutions and small electronic money institutions be reformed?**

   Please see our response to Q4.

7. **How, if at all, might the registration requirements for account information service providers be reformed?**

   Please see our response to Q5.

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

   As HMT will of course be aware, we are awaiting JROC’s roadmap/recommendations, which will be central to the future of Open Banking. We anticipate the JROC report to include a number of relevant issues including (but not limited to) liability/dispute resolution frameworks, anti-fraud measures, and the Long-Term Regulatory Framework. Given it is not prudent or appropriate to presuppose the details of the report, UK Finance will submit a further response, in the form of an addendum, to this call for evidence (specifically on Open Banking) once the report has been released and the industry has had a suitable amount of time to consider the contents.

   In the meantime, please find below feedback on issues we do not believe will be in scope of the JROC report.

   General comments

   Holistic approach to 'alternative payment methods’

   JROC's work is focussed on and limited to Open Banking (i.e. the provision of AIS and PIS) and so it will not take account of other 'alternative payment methods' (APMs), both current and emerging, for example: the use of 'pay by bank' (which does not necessarily need to involve PIS), 'buy now,

pay later' (which is not really a payment method as such, rather the provision of credit), and electronic wallets (where payments are made from one person to another person, say a consumer to a merchant, by transfers between e-money accounts. The PSRs review should allow for APMs and further developments in this field and the PSRs themselves should approach such APMs on the basis of payment-rail neutrality, i.e. all types of payment methods should be treated in the same fair and even manner. This should apply from a PSU perspective as well as from a PSP perspective, i.e. the rights afforded to PSUs should be the same across different payment types, except where differences are appropriate and justifiable. The application of rights afforded to PSUs across payment types must also strike a fair balance on liabilities and be underpinned by sustainable commercial models for all parties.

Corporate PSUs

Corporate PSUs do not need the same rights and protections as consumers: this as a key principle needs to inform the future development of Open Banking. There are various ways in which this principle could be applied in practice to the current provisions in the PSRs, e.g. the need to provide access to TPPs at all, around the basis on which access to TPPs is provided and around the application of SCA. Beyond flagging this principle here, we will leave more detailed consideration of this to the JROC.

Specific provisions

Payment account

Some members believe that consideration should be given to potentially clarifying the scope of application of the TPP provisions, which currently apply to all "payment accounts" which are accessible online, irrespective of their underlying functionality (and limitations therein).

FCA notifications

We are not convinced on the benefits and/or proportionality of the obligations on PSPs to submit NOT003 AIS/PIS denial and also NOT005 Problems with a dedicated interface (SCA-RTS Article 33(3)).

9. **How, if at all, might the registration requirements or wider regime for agents be reformed?**

The use of agents by firms to carry out activities on their behalf is a well-established model that works well in this and other sectors. Agent firms can be a cost-effective way for principal firms to access new markets and offer innovative services.

As ever, striking a balance between the registration regime providing appropriate assurance vs the risk posed of non-authorised agents is key, and the authorisation regime should not be an obstacle to agent firms supporting the sector due to the innovative tech and services they can provide.

Principal firms retaining responsibility for the activities that agents carry out should help ensure that regulatory standards are maintained, but an area that we feel may be helpful to review or provide further guidance on is with regards to the level and type of oversight that is required by principal firms to achieve the requisite level of assurance. With the Consumer Duty and other regulatory changes raising the bar on the expectations between firms and their third parties, more clarity on information sharing, monitoring, contractual rights and obligations will help firms navigate this area of increasing regulatory focus

In addition, the concepts of agent and distributor are currently limited to payment services and e-money issuance respectively. However, we question why banks are not also able to appoint third parties as their agent or distributor.

Information requirements for payment services

10. **Is the current framework for the provision of information to payment service users effective? If not, how should its scope change?**

We believe that the current information requirements in the PSRs could be modified to ensure that PSUs are receiving the right information, at the right time, and in the right format, in order to avoid

an overload of information which could be detrimental to achieving desirable customer outcomes. This approach would also ensure more alignment between the information requirements in the PSRs and the consumer understanding outcome under the new Consumer Duty.

- **Prior general information for framework contracts (a less prescriptive approach) -** Currently under regulation 48, PSPs are required to provide (rather than 'make available') the PSU with the information specified in Schedule 4 of the PSRs before they enter into a framework contract. Our view is that the information required under Schedule 4 and the manner in which it has to be provided is overly prescriptive and that PSPs should be allowed to adopt a more flexible approach: this would be facilitated by moving the detailed requirements from the PSRs to the FCA's Approach Document (or whatever else will replace this). Currently the easiest method of complying with the obligation - by including the prescribed information within the framework contract as contemplated under regulation 48(2) – has led to overly convoluted terms and conditions which in most cases are unlikely to be read by the PSU. For example, Schedule 4, paragraph 2 requires PSPs to provide information about the maximum execution time for the payment services to be provided, a reference to the time of receipt of the payment order and the cut-off time, and the form and procedure for giving consent to the execution of a payment transaction and for the withdrawal of consent. For PSPs who provide current accounts, what this means in practice is a requirement to include lengthy tables within terms and conditions that provides this (very detailed) information covering each type of payment the PSU can make with their current account (cash, card, electronic payments). Our view is that such information would be better delivered by allowing PSPs to meet their requirements by instead directing PSUs to where this information can be found e.g. on their website (which would meet the 'make available' requirement).
- Allowing PSPs to adopt a more flexible approach in relation to what and how this information is provided would enable them to deliver the right information, at the right time and in the right manner. PSPs typically use 'layering' to help build up a customer's understanding of their products, services and terms and conditions, as well as different parts of their website in order to deliver common information (e.g. around access to FSCS and FOS). This suggestion would also be in line with the FCA's objective under the new Consumer Duty to have financial services firms present information in a consumer friendly and easily accessible manner. To enable this more flexible approach, there will need to be a change in the default position in the PSRs; from all information being "provided" to the PSU, with certain exceptions where information can be "made available", to a default position where all information is "made available" or "communicated", with clarity on certain specified items which need to be "provided". The requirements of the PSRs no longer need to be as prescriptive given the FCA's general principles including Principle 7: Communications with clients ("*A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading*.") and the new Consumer Duty. This approach is also reflective of changing customer habits: customers who are more digitally active tend to engage with transaction information as and when they require it. This means that the existing requirement to 'provide' statement information often results in little customer engagement and does not satisfy customer needs.
- **Changes in contractual terms -** The requirement under regulation 50 to notify customers of any changes to the framework contract and any Schedule 4 information with a minimum of two months' notice, even where the change is favourable to the customer, can be disproportionate, inflexible, and a hindrance to innovation. While this requirement has been slightly 'modified' through FCA guidance in its Approach Document (in relation to the addition of new payment services which do not change the terms and conditions applying to the existing payment services), the two sources are not wholly aligned and this leaves PSPs erring on the side of caution, meaning that changes which may be favourable to customers cannot be introduced quicker than 2 months (and must be personally notified). Similarly, changes to basic, static information (as is required by the Schedule 4 requirements), such as contact details, complaint details, and details of regulators, as well as execution times

(changes to which may not be within a PSP's control) do not necessitate 2 months' notice, and perhaps not even personal notice at all. In addition, the greater flexibility that applies to interest rate increases under BCOBS could be applied more widely, and the interest rate provisions themselves could adopt this proportionate approach (i.e. notification of interest rate reductions is only required if the balance is above a certain threshold, e.g. £100 or £1,000). The requirement to provide notification of all such changes is therefore often disproportionate, costly, and of very limited benefit to customers, who rarely look to the framework contract for this information in any event. By way of contrast the notice period for changes to credit card terms and conditions is usually shorter at 30 days.

- **Corporate opt-out** – The corporate opt-out (COO) available under regulations 40(7) and 63(5) of the PSRs is extensively used in the corporate context, however, we believe that further improvements could be made to fine-tune its application:
    - **Definition of 'micro-enterprise'** – the definition of 'micro-enterprise' needs to be simplified and updated to address practical concerns. The current definition is taken from an EC Recommendation from 2003: post-Brexit a more UK centric definition should be used**6**. In doing so, we would also suggest that any change to the definition of "micro-enterprise" should enable PSPs to make an assessment of an enterprise with reference to the corporate group of which an entity in question forms part. For example, if a large group of companies has one subsidiary which technically meets the definition of a micro-enterprise, the PSP should be able to take the group data into account when considering how the entity should be classified. In addition, the combination of the PSRs test (at the point of concluding the contract) and the FOS eligibility test (either at the point of concluding the contract or at the time of the complaint), in effect creates an ongoing monitoring obligation for PSPs which is disproportionately onerous. This 'dual test', combined with the EC definition which requires PSPs to undertake an assessment of the annual turnover and/or the balance sheet total of their customers (so as to ensure it does not exceed €2 million) and of the number of people employed (fewer than 10), as well as the fluidity of the manner of engagement of staff (no longer just 'employees' but also contractors and other workers creating uncertainty as to who should be included in the count to 10), creates unnecessary complexity and real compliance costs without achieving the right outcomes.
    - **Extending the scope of application of the COO** – the rationale for the COO over all of Part 6 (Information Requirements) remains valid and strong and should be extended to any new information requirements folded into the PSRs (for example from CBPR2 or the PARs). The rationale for the COO over certain provisions in Part 7 (Rights and Obligations) also remains valid and strong and should be extended to other provisions in Part 7. An example would be the ability to use the 'OUR' charging code in the context of intra-UK non-sterling transactions (covered in more detail in our response to Q17).
- **Miscellaneous**
    - **Remove legacy EU centric provisions**: there needs to be a tidy up in terms of updating legacy EU centric provisions that currently persist within UK regulation relating to customer information requirements. By way of example, when setting out the information that must be provided to customers in relation to card-based currency conversions under Article 3A of the UK CBPR, it is currently required that the PSP "*shall express the total currency conversion charges as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the European Central Bank*".

[6] It is not clear what this definition should be (examples which could be used are the definition of "small company" or "micro-entity" under the Companies Act 2006, although we note their different turnover/balance sheet thresholds as compared with the existing definition of micro-enterprise) but our view is the term should be applied consistently across the UK's financial services regulatory regime.

- **Move to digital**: there are currently numerous references to paper statements under the PSRs (e.g. in regulation 53) and we query the purpose and value of statements for the majority of customers who prefer to view their statements online or in their banking app. Digital statements should now be the default, with the option for PSUs to opt-in to paper statements (rather than the other way round, as currently) as is the case under Article 24(5a) of MiFID2. We recognise, however, that there may still be a need to retain the requirement to provide paper statements in certain cases, such as for customers who are in overdraft position, or customers who have incurred fees and charges over the period, or those who are not digitally engaged. There are also concerns over the environmental impact of paper statements and the potential for them to be used in social engineering scams. Linked to the move to digital, monthly statements may not always be the most appropriate level of frequency and there should be greater flexibility for PSPs to be able to agree with the PSU a different level.

- **PISPs/AISPs**: We believe there should be more general clarity around contractual arrangements for both PIS and AIS and potentially specific provisions that cover the information requirements that apply to both. The binary approach of "framework contract" or "single payment contract" doesn't neatly fit these services as they are defined. For PIS, we believe that the information obligations that come with framework contract arrangements are not well suited to PIS use cases, in particular variable recurring payment arrangements and embedded payment scenarios. They don't reflect PIS business models (where the main customer relationship might be with another PSP) and impose obligations to provide transaction information to the customer in a durable medium that the customer will be receiving from their ASPSP in any event. We would advocate for a more proportionate regime/approach that avoids overlap in provision of information and reflects the different nature of the customer relationships a PISP will have as compared with an ASPSP. Also of note, regulation 60 is helpful in defining the requirements for RAISPs, but (i) it needs to be amended so that it is clearer that it should also cover PIs/EMIs and credit institutions carrying out AIS, and (ii) its not evident why minimum standards included in the contract cannot be set more clearly, rather than leaving it to PSPs to define what is "relevant" in Schedule 4. Also, the definition of "*framework contract*" (or, noting our comments above, the equivalent for PISPs) should make clear that it also covers PIS in order to prevent confusion within the payments industry, for example through a simple amendment such as the following (additional text underlined): "*a contract for payment services which governs the future <u>initiation and/or</u> execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account*".

- **Impact of new technological developments**: There are new technological developments within the payments industry, and it would be helpful to consider the impact of the current PSR information provisions on those: Under the PSRs, PSPs have an obligation to include the information they receive with a payment on the statement. The NPA and renewed RTGS are both being built using the new international ISO 20022 standard. ISO 20022 is capable of carrying additional data with a payment to those carried today. The purpose behind the additional data under the new standards is to help firms identify and tackle fraud, and to know which payments to prioritise (e.g. purpose codes for property transactions made via CHAPS). It would be helpful to consider whether there is a need to provide further clarification of the PSR requirement in light of the new standards, in order to clarify how much of this additional data is required to be included on the customer statement. Otherwise, there is a risk that the default position will be a requirement to include information which is not helpful for customers and results in an adverse impact on customer understanding.

11. **Are there particular changes that you would advocate to the Cross Border Payments Regulation in relation to the transparency of currency conversion, and what would these entail?**

    This review presents an opportunity to review the Cross Border Payment Regulation in its entirety in order to assess whether all of the requirements remain appropriate in the UK. If requirements remain appropriate, we agree that they should be incorporated within the PSRs.

    This review also presents an opportunity to clarify that although HMT confirmed in its explanatory memorandum that the Article 3(5) requirement on electronic messages (which came into force in Europe in April 2021 (i.e. post-Brexit)) would not be onshored, the onshoring legislation didn't specifically remove them. These should be removed in the legislation (members were supportive of the decision not to on-shore these provisions and saw limited value in the alerts). As referenced earlier, it also presents an opportunity to consider whether the use of the ECB rate as the reference rate remains appropriate post-Brexit (although it is not clear what the alternative should/could be). More generally, UK Finance members would caution against further significant changes to the transparency requirements.

    Please also see our responses to Q2 and Q10.

Rights and obligations in relation to the provision of payment services

12. **What has been the experience of a) providers and b) users/customers in relation to the termination of payment services contracts? Does the existing framework strike an appropriate balance of rights and obligations between payment service users and payment service providers, including but not limited to a notice period applying in such cases?**

- UK Finance strongly supports the balance of rights and obligations as set out in existing payments regulation. We are not aware of widespread consumer concern on the termination of accounts, although there have been some high-profile cases recently. We caution against changes which may have unintended consequences on a PSP's ability to manage risks including fraud and other illegal activity such as money laundering and terrorism. This would significantly cut across public policy objectives.
- Our members recognise the importance of customers not having their accounts, services or contracts terminated inappropriately or unfairly. They are keen to work with the FCA in relation to issues such as account blocking or freezing, which was referred to by the FCA in its recent Dear CEO letter to payment firms. Firms are committed to investment in new technology and process improvements to manage, in the best interests of all customers, illegal activity. We welcome discussion on how the existing requirements in the PSRs address the needs of customers, both individual consumers and merchants, through the Consumer Duty lens.
- UK Finance members believe the existing framework does strike an appropriate balance of rights and obligations between PSUs and PSPs, including the current notice period requirements in regulation 51. There is also sufficient existing protection under the Consumer Rights Act and the Equality Act. It is worth noting that the FCA's new Consumer Duty obligations, relating to the withdrawal of products, will strengthen the regulatory regime and general Financial Ombudsman Service rights.
- We therefore strongly disagree with any new regulatory requirement which:
    - Would limit a PSP's right to be able to terminate a contract (which PSPs can currently do without any reason, provided 2 months' notice is given);
    - Would restrict a PSP's ability to immediately terminate contracts to only where criminal activity had taken place.
- In the normal course of events, customers should have good communication about their accounts and the notice period should be served before their account is terminated. However, PSPs must retain the right to disapply the notice period when the customer is suspected of engaging in illegal activity. PSPs use sophisticated detection processes with a number of risk indicators to identify

potential illegal activity, and in each case will need to make a judgment on whether to terminate an account. This judgment balances the rights of the customer against the risk of the potential illegal activity continuing (and causing harm to others, which could include other consumers (abusive payments messaging) or staff (altercations in branches etc.).

- Moreover, payments by nature operate in a network environment, and each entity will have obligations to other firms in the payments chain. As it has been a long-standing priority for the payments industry to identify and restrict the use of payment methods for illegal purposes, often in conjunction with law enforcement bodies, this means that a number of these obligations relate to identifying and stopping illegal activity. These network obligations help to prevent illegal activity in a range of areas such as money laundering, age-restricted content and gambling, and should not be undermined.
- If a PSP were required to satisfy a criminal standard of evidence in order to terminate a contract, and thereby avoid incurring penalties or complaints to the FOS, this would put PSUs and members of the public at risk and create a conflict with financial crime regulations. Moreover, giving the customer notification and reason for the closure of the account may inadvertently breach rules on 'tipping off' customers by revealing information which is likely to prejudice any resulting law enforcement investigation.
- An additional important area in which PSPs need to exercise judgment on terminating accounts is credit risk. If PSPs are unable to close accounts on this basis it will have a major impact on the onboarding process, as they will need to be much stricter on creditworthiness assessments. This will in turn lead to increased costs for PSUs and merchants and will have far reaching consequences for any liability frameworks. Similarly, flexibility is required for other commercial decisions – e.g. continued reimbursements following fraud and gambling-related losses which exposes the firm to associated liabilities.

13. **With reference to paragraph 31 of the accompanying review, do stakeholders have any feedback on the government's view:**

- **that, as a general principle, a notice period and fair and open communication with a customer must apply before payment services are terminated?**
- **that the regulations and wider law operate here as set out under paragraph 29?**

Please see our response to Q12.

14. **How and when do providers cease to do business with a user, and in what circumstances is a notice period not applied?**

Some examples of when PSPs will terminate contracts without the notice period include (non-exhaustive):

- When PSPs are legally required to close the account.
- When the customer has (or is reasonably suspected to have) carried out illegal or fraudulent activity on the account.
- When the customer has committed a serious breach of terms and conditions on the account.
- When the customer has used threatening or abusive language towards staff or a third party.
- When the customer has failed to pay an overdrawn balance on the account.
- When the customer has not provided information required for identification.
- When the PSP reasonably considers they may be exposed to action from any government, regulator or law enforcement agency.
- When there is a change in product features and/or target market which results in a change to the product or service eligibility criteria, meaning the product is no longer suitable for the customer

15. **How effective are the current requirements in the PSRs, notably under Regulations 51 and 71 – are these sufficiently clear or would they benefit from greater clarity, in particular to ensure that notice-periods are given and customer communication is clear and fair?**

    Some examples of when PSPs will block a PSU's account (i.e. suspend cards or use of banking apps) include:

    - When the PSP has legal or regulatory obligations to meet.
    - When the PSP is concerned about security.
    - When the PSP believes it is necessary for protection against fraudulent activity.
    - When there is a significant increased risk of the customer not being able to repay an overdraft.
    - When the PSP is informed that the customer is deceased or when there is a safeguarding concern over the mental capacity of the account holder.

    On occasion, the PSP will require the customer to provide information to help meet anti-money laundering, financial crime, sanctions and other legal and regulatory requirements. If this information is not forthcoming, the PSP may need to block the account to avoid their own breach of regulatory requirements.

    In the normal course of events, the PSP will inform the PSU in advance of blocking (including reasons) unless this would compromise reasonable security measures, or it is unlawful to do so. If a PSP is unable to inform a PSU or make information available to the PSU in advance, the PSP will inform the PSU immediately afterwards.. The exception to this is where it might compromise reasonable security measures (see answer to question 12). The PSP will then lift the block once the reason for it has been resolved.

16. **Should there be additional protections for payment service users against the termination of contracts? Should anything be specific to protect their freedom of expression – e.g. to ensure that adequate (or longer) notice is given in such cases, and what communication requirements should apply?**

    Please see our response to Q12.

Wider considerations in relation to the provision of payment services

17. **What provision, if any, should the regulatory framework make regarding charges for payment services?**

- We believe that the regulatory framework should make allowance for commercial models and charges to develop. As stated in the answer to Q1, payments cost money to provide and require the development of sustainable commercial models. Moreover, the ability to develop commercial models allows for payment ecosystems and networks to develop. However, the development of commercial models may give rise to competition risk, so this is an area where involvement of regulators is critical. As an example, the regulatory framework for Account-to-Account Retail Transactions including an extension of open banking payments beyond PSD2 should accommodate commercial models and that will be helpful in the development of an open banking payments system.
- Post-Brexit, for one leg-out transactions to or from the EEA (except for SEPA payments) the 'OUR' charge code is permissible, as these payments are no longer subject to the shared charging obligation in regulation 66(2). However, the position for intra-UK payments is that the 'SHA' charge code is mandatory for all intra-UK payments in any currency. We believe that amendments should be made to allow other charge codes to be used, i.e. OUR or even BEN, either following disclosure to the PSU and agreement to the payment transaction on that basis or under an extended COO. There is also a more general case to allow OUR for intra-UK non-sterling transactions, particularly in the corporate context where it would facilitate (although not guarantee) that the beneficiary receives the full amount. This would support the government's growth and competitiveness agenda, by allowing PSPs the flexibility to meet demand from certain clients who would prefer to accept all

charges themselves (i.e. charge code 'OUR'), thus limiting the impact on beneficiaries. Examples of transactions where this would be beneficial would be where an insurance company is paying a claim or an international business is paying pension or salary payments to (retired) employees. Another example is where a corporate is purchasing a shipment of goods e.g. oil in USD, but requires the full value to reach the beneficiary before goods are released.

18. **Does the existing framework (of the regulations) strike an appropriate balance of rights and obligations between:**

- **Sending and receiving payment service providers?**

UK Finance does not believe that the risk-based approach issue is a question of balancing of rights and obligations. We have the view that changes are needed to provide extensions to payment processing timeframes for both inbound and outbound faster payments, recognising that both sending and receiving PSPs have differing vantage points and opportunities, and should be given parity of treatment to enable prevention of fraud to their consumers.

- **Account servicing payment service providers and payment initiation service providers/account information service providers?**

Please see our response to question 8

Fraud

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

Our views on this are reflected in our consultation response to the Payment Services Regulator dated 9 December 2022 and in various papers, roundtables and written responses to questions posed by HMT as part of our discussions on adoption of a risk-based approach from June 2022 to February 2023.

There is an absence of a clear legislative framework to enable freezing and repatriation of funds to victims of fraud. The current framework for firms to respond to consumer APP fraud claims is governed by an industry developed voluntary APP Best Practice Standards. In addition, adoption of the BPS platform does not cover all PSPs. The PSRs do not expressly provide a means for Firm A to repatriate funds to Firm B to reimburse a victim. BPS participating firms have been proceeding at a legal risk in doing so and the status quo enables considerable inconsistency in approach and outcome. Activity is currently managed through terms and conditions and indemnities where possible to do so; this is also contributing to delays in reimbursement for victims. This problem is compounded where victims are not entitled to reimbursement. We would encourage HMT to bring forward an amendment to the PSRs to provide an obligation on PSPs to make reasonable efforts to recover funds where a fraud has been confirmed.

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

Within ecommerce there are soft declines and natural consumer interaction points with the PSP when a card payment is declined.

For Faster Payments (i.e. transfers from one payment account to another), our views on this are reflected in various papers, roundtables and written responses to questions posed by HMT as part of our discussions on adoption of a risk based approach from June 2022 to February 2023.

On 17 March 2023, UK Finance made the following proposals to HM Treasury to give effect to the adoption of a risk based approach to both inbound and outbound Faster Payments:

- **Changes to allow PSPs to 'pause' a payment transaction**: UK Finance believes that amendments are needed to regulations 86 and 89 of the PSRs to insert an exemption which disapplies the current processing timeframes for both inbound and outbound payments where

the PSP reasonably believes there is a heightened risk of fraud associated with the payment. UK Finance proposes that these amendments should be accompanied by reviews and updates to the existing FCA guidance within the Approach Document, in order to allow appropriate flexibility by managing the application of timeframes through regulator managed guidance.

- **Obligation to communicate with affected customers**: Where processing is delayed in line with regulations 86(1) or 89(1) and reliance is placed on the extended timeframes in cases of heightened fraud risk, there should be a requirement to communicate with the affected customers. UK Finance suggests that an obligation is included that mirrors the provision in regulation 82(1) that requires communication of the delay and basis for the delay. That requirement should contain the same caveat in regulation 82(4) which enables a payment service provider to not notify where such notification would otherwise be unlawful.
- **Status of released payment**: If the PSP subsequently executes a transaction, that payment transaction should be treated as if it were executed without payment delay, i.e. there should be no PSU detriment for interest purposes as a result of the payment transaction being held.
- **Scope**: The scope of the proposed amendments should be limited to payment transactions executed where either the payer or the payee's PSP is in the UK and the payment transaction is in GBP. This should ensure that it covers so-called one-leg out transactions (e.g. where the payment is being made to someone overseas), while ensuring that it does not prejudice the UK's continuing participation in SEPA (as the proposed provisions do not extend to transactions denominated in euro or in any other currency than sterling) which is a priority for UK Finance members and more generally, the UK.
- **Consolidation**: Lastly, the proposal touches upon a number of different provisions governing payment processing and ancillary matters, however, UK Finance proposes that all the different elements of the new provision should be consolidated in one place.

21. **In relation to fraud, whether unauthorised or authorised, is there a need to**

A. complement rules with data sharing requirements?

We would welcome the introduction of an explicit requirement on the need for data sharing in cases of authorised payment fraud with PSP-to-PSP transactions. There is currently no explicit requirement for data sharing between PSPs to recover funds in cases of authorised payment fraud.

In cases of unauthorised fraud, the need to share data is implied by the requirement in the PSRs to make reasonable attempts to recover funds. In addition, the new 3DS protocol can already capture additional data for the e-commerce card payment environment. As this is a new protocol and has yet to mature we do not see the need for additional data sharing requirements within the ecommerce environment at this time.

Should data become mandated there is a critical need for integrity and consistency monitoring to support machine learning models and avoid unintended consequences (such as greater unnecessary blocks or exceptions for genuine payments).

UK Finance also notes that the obligation to share data would need to be designed to make clear which entities can (or must) share data, and with who data can (or must) be shared.

Strong Customer Authentication

B. further reforms be made to make Strong Customer Authentication (SCA) work more effectively and proportionately?

We believe that there is a strong case for reforms to the SCA regime to make it work more effectively and proportionately. We have set out below our views on how the SCA regime could be reformed, both high-level comments and suggested detailed changes to specific provisions in Appendix A.

High-level comments

We have set out here our high-level comments on the current SCA regime and how it should be reformed:

- **Framework** – the current SCA regime essentially comprises: (1) regulation 100 in the PSRs; (2) the UK SCA RTS; (3) the relevant parts of the FCA Approach Document; (4) supporting EBA Opinions and PSD2 Q&A; and (5) UK Finance's SCA Industry Guidance (December 2022). We believe that:
- The core requirement in regulation 100 of the PSRs is set at the right, high level and subject to one comment should be retained as is.
- The UK SCA RTS and any relevant, helpful parts of the supporting EBA guidance should be carried forward into and combined with the existing relevant parts of the FCA Approach Document in a new SCA section of the updated FCA Approach Document, with the FCA designating certain parts of the RTS as rules or guidance as appropriate (e.g. the exemptions should be designated as rules). This would also enable a more agile supervisory approach from the FCA, as this SCA section could be updated independently.
- UK Finance's SCA Industry Guidance could be given greater weight, with ideally the FCA endorsing it.
- **Approach to change** – the SCA regime has not been in place for long, so change for change's sake should be avoided: furthermore, change should be guided by the overall objective of reducing the risk of unauthorised transactions and fraud and by evidence, not expectation. For example, data gathered by UK Finance indicates that the risk of fraud is four times greater with the use of OTPs sent to a mobile device than in-app authentication.
- **Future flexibility** – the SCA regime should also allow for future flexibility to allow PSPs to stay ahead of fraudsters.
- **Outcomes focussed** – the SCA regime should also allow for PSPs to depart from the strict requirements where to do so will achieve a better outcome. For example, data gathered by UK Finance indicates that it is much easier for fraudsters through social engineering to work around the Knowledge and Possession factors – presently the requirement for there to be two different SCA factors precludes PSPs from using two Inherence factors to meet the SCA requirement (they may use a 2nd Inherence factor presently, 'layering' this on top of another factor like Knowledge or Possession, but they cannot use it to meet the SCA requirement). To do this, either the definition of "Strong Customer Authentication" should change in the PSRs when revised or an exemption should be permitted to allow (a) a more general risk-based approach (the current TRA is overly limited); or (b) a PSP to use a 2nd Inherence factor (instead of Knowledge or Possession).
- **Different cohorts of customer** – this outcomes-focussed approach would also enable PSPs to cater more specifically to particular, perhaps much smaller cohorts of customer such as vulnerable customers, where the application of the rigidly defined SCA poses real challenges in practice.
- **SCA as friction in the customer journey** – customers are equally concerned about fraud themselves and so they see friction in the customer journey positively too: such friction can also help automated fraud tools operate behind the scenes to detect potential instances of fraud, so a drive to a completely frictionless customer journey in all cases is not supported.
- **Liability shift** – PSPs and their service providers (such as acquirers and gateway providers used in card transactions) should be able to agree between themselves when liability shifts from the card issuer to the merchant via the acquirer, say for the purposes of compensating the payer under regulation 77(4). This might mean for example that the requirement in regulation 77(6) should not apply in these instances and/or the obligation on the card issuer in regulation 100 should be switched off. Again the new framework should allow for this, by being less prescriptive and/or having guidance to this effect in the FCA's Approach Document.

- **Parity** – Members have reported that some PISPs would prefer to see higher SCA exemption thresholds for payments initiated through PISPs than for payments initiated by PSUs directly. However, our strong view is that the rules on SCA should apply equally to all PSPs (whether an ASPSP, AISPs or PISPs).

Issuance and redeemability of electronic money

22. **Are the requirements regarding issuance and redemption of electronic money still appropriate?**

    No Response

23. **Noting the intention to commission an independent review in due course, do you have any immediate observations on the efficacy of the operation of the Payment and Electronic Money Institutions Insolvency Regulations to date?**

- Noting the intention to commission an independent review, we have at this stage restricted our observations on the safeguarding regime set out in the EMRs and PSRs and on the special administration regime (SAR) in the PEMIIRs to immediate, high-level ones (references to the PEMIIRs are to the Payment and Electronic Money Institution Insolvency Regulations 2021).
- First, we would strongly advocate that (a) the scope of this independent review include not only the efficacy of the operation of the PEMIIRs, but also the efficacy of the safeguarding regime set out in the EMRs and PSRs: the two must be considered together, and (b) this review be conducted urgently, involve all relevant stakeholders and be acted upon swiftly: the current position following the Court of Appeal's decision in Ipagoo has created huge uncertainty for all involved. In particular, the stakeholders with which this review should be engaged must include: (a) the community of providers of bank account services to payment and e-money institutions (i.e. banks), as they are concerned by any unintended consequences for them of imposing trusts over relevant funds held (e.g. whether this could impose any operational constraints and/or expose them to additional risk as a result of funds being capable of being 'traced' under trust law), and (b) insolvency practitioners, so that considerations of insolvency law, of the practical operation of an administration or insolvency, and of the risks to which insolvency practitioners are potentially exposed, are all taken into account.
- Secondly, we would comment that while the adoption of a safeguarding regime based on CASS and of the PEMIIRs based on the Investment Bank Special Administration Regulations 2011 (IBSARs) may be attractive, in practice there is a significant difference in the underlying assets (under CASS, investments, and under EMRs/PSRs, money held for the purpose of making payment transactions), which needs to be accommodated and provided for within the relevant regime and regulations. Money (i.e. 'relevant funds') held for the purpose of providing payment services and/or received in exchange for e-money will typically have accounts, cards and other payment instruments associated with or attached to them, be used and replenished frequently (intra-day as well as daily), and be used for regular payments (direct debits, standing orders and future card payments), the non-availability of which will have far-reaching consequences. Ensuring non-depletion in value needs to be balanced with continuing access to all of these uses of the relevant funds held under the safeguarding regime and the SAR for distressed payment and e-money institutions, particularly where the users are 'vulnerable customers' or potentially otherwise 'unbanked' users.
- Thirdly, it may be appropriate for HMT and the government to review wholesale the protections afforded to users in the event of an insolvency of a PI/EMI, considering likely consumer harm, including whether:

    (a) there should be some overriding objective of 'continuity of service' (rather than simply the return of funds), given the nature of the services involved (which are intended for the purpose of making payment transactions);

    (b) the concept of safeguarding should adopt features of other sector schemes such as the Financial Services Compensation Scheme (FSCS) which have worked well for customers. These features include the guarantee of timely return of customer funds in full, up to a specified limit, without being compromised by administration or other fees. (At the same

time, we also note, as per para 10.16 of the FCA's Approach document that PIs and EMIs should be clear in their communication and should not suggest funds are protected under FSCS); and/or

(c) the protective elements of such a scheme can be available to customers of PIs and EMIs (as they are not themselves 'eligible claimants' under the FSCS), and if so, how.

- We are aware that ensuring customer money is safe remains a top priority for the FCA. This was evident in the 'Dear CEO' letter which was issued to payment firms on 16 March 2023. Whilst the FCA outlined in this letter some of the 'compliance gaps' it may have seen, it would be helpful to the industry if the FCA could follow up on this with an update on its published views to provide further clarity on points within the Approach document, namely;
- what firms should be doing with respect to the set-up of safeguarding accounts – for example, banks are regularly provided with the FCA's template safeguarding letter. However, this refers to the establishment of a trust, which post-Ipagoo is incorrect, and payment and e-money institutions are often incredibly reluctant to make any changes to the letter for fear of not meeting the FCA's requirements in this respect;
- whether UK payment and e-money institutions should be safeguarding funds held for non-UK customers – our understanding of the FCA's approach is that such firms are not required to safeguard funds held for non-UK customers (the FCA's Approach Document, paragraph 10.26 is not unequivocal on this point, though this is a commonly held view in the market and more importantly the approach the FCA has adopted in recent insolvencies of APIs/EMIs (not least given the issues of funds flowing outside of the UK);
- and whether a UK payment institution that is concerned with transactions between a non-UK (and non-EEA) payer and a non-UK (and non-EEA) payee, where those transactions are provided by that firm or its agent from a non-UK (and non-EEA) jurisdiction, is required to safeguard those funds – and in connection with that, whether the 'characteristic performance' test (explained in European Commission communication 97C 209/04) should be applied in determining the place of performance for such purposes. Paragraph 10.26 of the FCA's Payment Services and Electronic Money approach paper is not unequivocal on this subject.

Miscellaneous

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

Major operational incident (MOI) reporting – we believe that there is scope for the FCA as part of its review when folding the EBA guidelines into the FCA Handbook on a more long-term basis, to provide clearer, more focused, and proportionate guidance as to MOI reporting, particularly as to the reporting of lower impact incidents within the 4 hour window, irrespective of the time of day.

Retention of corporate opt out – members strongly believe that the corporate opt out should be retained so that PSPs and PSUs that are not consumers, micro-enterprises or small charities have the flexibility to negotiate applicable terms between them according to the specific services provided by the PSP and the business needs of the PSU.

Access To Cash - HMT will be aware that UK Finance has been working closely with the government and regulators on the issue of access to cash. Bank branches are needing to close but consumers and small businesses do still require both access and deposit making facilities. In particular, we have been working with industry and other stakeholders on innovative solutions to facilitate the deposit making options. Some hurdles have been encountered relating to automated depositing of cash and coin with third parties. This is attributed to regulatory restrictions from the PSRs (cash over the counter requirements for example). We want to flag this issue now to HMT so that we can continue to work with other stakeholders, particularly Cash Access UK Limited and its members, on defining what it might be useful to review within the regulations in order to unlock greater opportunity for cash deposit innovation in the UK.

Appendix A: Specific changes relating to Strong Customer Authentication

We have set out here our suggested detailed changes to specific provisions.

General requirements under the UK RTS

- **Audit requirements** – the audit requirements in Article 3 (and in particular, the audit requirement where a PSP makes use of the TRA in Article 3(2)) should be removed. As while this may have been useful upon the introduction of SCA, other parts of the payment services regime (indeed, all other conduct of business requirements) are not subject to specific audit requirements (rather the onus is on PSPs to ensure compliance with applicable provisions).
- **5 minute rule** – PSPs should be able to determine themselves the appropriate inactivity period for the purposes of Article 4(3)(d) based on the customer profile and a risk based approach or at least be able to apply the Article 17 exemption.
- **Dynamic linking -** the RTS Article 5 dynamic linking requirements create inefficiencies and frictions when applied in a corporate context. Allowing the RTS Article 17 'corporate exemption' to apply to dynamic linking would overcome these issues.

Exemptions

- **General (exemption for non-payment initiation)** – presently, with the exception of Article 10 and 10A, all of the exemptions deal with payment initiation only: there should be exemptions for the other limbs requiring SCA, i.e. which would apply to regulation 100(1)(a) (access to payment accounts) and 100(1)(c) (remote actions where there is a risk of fraud).
- **Article 17 (secure corporate protocol) -** there is no general COO, even for highly sophisticated corporates and financial institutions. For these customers, SCA is inherent in the use of PKI and other highly secure means of communication and within this environment, the strict SCA requirements should not apply. Furthermore, as currently drafted Article 17 is limited to "legal persons" only, so excluding use for partnerships and sole traders.
- **Article 18 (TRA)** – Article 18 of the SCA-UK RTS permits PSPs not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the PSP as posing a low level of risk and where certain other conditions set out in Article 18 of the UK SCA- RTS are met. Our members are of the view that fraud targets should be linked to a TRA that is outcomes based and not based on the value thresholds currently outlined in the SCA-UK RTS. Additional requirements place an obligation on PSPs to notify the FCA of movements through the fraud rate tables. We note that portfolios with specific characteristics, for example 1 fraud occurring on a high-net-worth customer, could have a disproportionate impact on the fraud rate calculation. We are of the view that the frequency of reporting could be adjusted to allow PSPs to monitor, analyse and adjust their strategies to minimise fraud losses, if the reporting requirement is necessary.
- **SCA exemption for Electric Vehicle (EV) charging -** A specific exemption from SCA for EV charging should be added to support the continued growth of EV charging, so contributing to the government's Ten Point Plan, as well as supporting business and consumers. Article 12 of the UK SCA RTS already provides an exemption for unattended terminals for transport fares and parking fees. Either this exemption could be extended (as it relates to transport and unattended terminals – aka charging points) or a fresh exemption could be added.

Appendix B: Consent for use of personal data

Reg 97 states:

- “Consent for use of personal data
    - **97.** A payment service provider must not access, process or retain any personal data for the provision of payment services by it, unless it has the explicit consent of the PSU to do so.”

Confusion has been caused by certain provisions in the PSRs that are in tension with certain provisions in the UK GDPR and/or seem to dictate a particular approach by PSPs to compliance with their separate obligations under the UK GDPR. The particular provisions in question are:

- Regulations 69(3)(g) and 70(3)(f), which require a PISP and an AISP, respectively, to "*not use, access or* store *any information for any purpose except for the provision of the [PIS/AIS] explicitly requested by the [PSU]*";
    - However, UK GDPR allows further use of personal data provided this is proportionate, there is a lawful basis for processing such data, and certain other tests are met to protect the individual’s rights. For example, it may be justifiable to further process data collected in order to develop enhancements to the product or to identify signs of fraud.
- Regulation 97, which requires that "A [PSP] must *not access, process or retain any personal data for* the *provision of payment services by it, unless it has the explicit consent of the [PSU'] to do so*".
    - The expectation that personal data will only be processed with ‘explicit consent’ is at odds with the UK GDPR’s ‘legal basis for processing’ framework under Article 6, which does not typically consider consumer agreement to receive a service under a contract to be ‘consent’. This confusion in the PSD2 text was flagged by the ICO in its 2017 submission to HM Treasury on PSD2 implementation. FCA also recognised the confusion, clarifying in its Approach Document at 8.53-.56 that the GDPR’s notion of consent should not be read across to the PSRs.

We recommend reviewing these provisions to better align them with the overarching data protection framework created under the UK GDPR and the Data Protection Act. It may ultimately be that these provisions can simply be deleted and reliance placed on the general, non-sector specific rules that these laws provide. However, we highlight that we are not recommending changing the policy such that TPPs can access customer data without the appropriate customer protections, rather, we recommend making *technical* fixes to better align the PSRs with the applicable UK data protection rules.