



Electronic Money Association

Crescent House

5 The Crescent

Surbiton, Surrey

KT6 4BN

United Kingdom

Telephone: +44 (0) 20 8399 2066

www.e-ma.org

Payments and Fintech team
HM Treasury
Horse Guards Road
SW1A 2HQ

By email: Modernisingpaymentservices@hmtreasury.gov.uk

6 October 2026

Dear Sir/Madam,

Re: EMA Response to [HM Treasury consultation on Modernising Payment Services Regulations](#)

The Electronic Money Association (EMA) has been representing electronic money issuers and payment service providers in the UK for over 20 years. Our members include leading global payments and e-commerce businesses, providing online payments, e money wallets, cryptoasset services, TPP and online banking payments, card-based products, electronic vouchers, and mobile payment instruments. A list of current EMA members is provided at the end of this document for reference.

The EMA is grateful for the opportunity to respond to HM Treasury's consultation on Modernising Payment Services Regulation. This consultation is a significant milestone for the UK payments and e-money sector; its outcome will shape the regulatory framework for years to come and will be central to the sector's continued ability to innovate, compete and support growth.

Yours sincerely,

A handwritten signature in black ink, which appears to read 'Thaer Sabri', is positioned above a horizontal line that extends to the right.

Dr Thaer Sabri
Chief Executive Officer

Electronic Money Association

EMA response

Introductory remarks: The UK can be rightly very proud of the success of its Fintech Sector, which is a significant economic generator of wealth and employment. What is not widely appreciated is that a high proportion of the Fintech Sector are Payment Service Providers (PSPs) regulated by the Financial Conduct Authority (FCA) as Electronic Money Institutions (EMIs) and Payment Institutions (PIs).

The regulators' original intent for the e-money regulations was to create a lighter-touch, proportionate regulatory regime to encourage competition into the payment sector. This has been a huge success; the UK's e-money and payment services regulatory regime has introduced much needed competition, lowered prices, and fostered innovation. The Sector is highly diverse, and boasts many innovative tech-oriented firms, each with a differentiated business-model, aimed at offering products and services to under-served niches of the market.

Several of these firms have grown out of this sector to become Unicorn Businesses - a Unicorn is an American term for a start-up business that quickly achieves a valuation exceeding one billion dollars. The UK has over 1,200 non-bank Payment Service Providers (NBPSPs), exceeding the number in all of the countries in the European Economic Area (EEA) combined.

It is in this context that the EMA urges HM Treasury to ensure that the MPR reforms do not erode this success through more, burdensome regulation, or unnecessary 'streamline' changes to the 'regulatory sandbox for innovation' that e-money has become.

An agile, modern and future-proofed regulatory regime should not come at the expense of forfeiting a regulatory environment that enables economic growth, innovation and competition.

Question 1: Which firm facing requirements should remain in legislation and which should be delegated to the FCA? Please explain your reasoning.

On the architecture of the payment services regime and delegation to the FCA

The consultation confirms the government's intention to achieve balanced delegation of payment services regime rules to the FCA, where flexibility and a more outcomes-based approach brings clear benefits, while preserving essential elements in legislation to ensure predictability and certainty. The EMA welcomes these as the general guiding principles for retaining rules in delegation vs delegation to the FCA. However, the consultation lacks detail of the FCA's future rule-making mandate, including the objectives and accountability framework that would support it.

In that context, the intended shift towards a more FSMA-style model of regulation - with regulatory requirements increasingly spread across legislation on the one hand and the FCA rules on the other, represents a significant structural change for payment services regulation from the status quo. This raises two key areas of concern.

First, a concern our members raise consistently is that delegation may in practice produce a more fragmented and less navigable regime than the one it replaces, despite the flexibility, predictability and certainty objectives set out above. Practically speaking, some of the payment services regime's success has been attributed to the rules primarily set out within a single, self-contained instrument. The FCA's Approach Document - also a self-contained document - has also been hugely successful as a source of guidance for e-money and payments firms, and to this day is considered a 'gold standard' when compared to guidance from any other European competent authorities. With parts of PSR-equivalent rules moved into the FCA Handbook, and likely dispersed across multiple sourcebooks, the concern is the regime would become more, not less, complex and opaque. This can add a meaningful burden, particularly for smaller EMLs and PLs without large legal and compliance functions, and a concern our members consistently raise as a reason against moving towards a more FSMA-style regulation.

Secondly, and more fundamentally, there is the issue of ensuring that the FCA's rule-making framework and objectives are set up for the regulatory environment that enables innovation, competition and economic growth of the UK's payment services sector. The intended delegation and replacement of requirements through the FCA's Handbook would - we presume - engage the FCA's existing statutory objectives, namely consumer protection, market integrity and competition, alongside its secondary growth and competitiveness objective and the wider "have regard" matters under Chapter 1 of Part 1A of FSMA. The concern is that greater delegation of rule-setting to the FCA creates a structural risk of more, not less, conservatism and overregulation: as a regulator, the FCA may tend to weigh, for example, consumer protection over its growth, competition and innovation objectives more heavily than the pursuit of government's objectives for the MPR programme intend. A related area of concern has to do with a question of regulatory accountability, in the context where policy making is essentially being transferred from legislators to the FCA.

Peers raised exactly these concerns in the House of Lords, during debate on separate reforms under the Financial Services and Markets Bill 2026 currently before Parliament, over the lack of parliamentary oversight accompanying the transfer of legislative requirements to regulators, particularly where there is little detail on the regime that would replace the one being repealed. We share these concerns for the MPR reforms also, and ask HM Treasury to set out how it will ensure FCA rule-making stays aligned with the programme's own stated objectives, including a modernised, clear, predictable and proportionate framework that supports innovation and competition, and what accountability framework will govern it.

Requirements that should remain in legislation

The EMA would welcome a consistent approach for retaining the following types of requirements in legislation:

- provisions that set or move the e-money and payment services regulatory perimeter;
- provisions that set out the core rights and obligations under UK's payment services regime, especially those that bind or are enforced by parties outside of the FCA's regulated population, including by the courts as well as insolvency practitioners.

The more technical or operationally detailed firm-facing requirements could, on the other hand, be reasonable candidates for delegation to the FCA.

Against this background, the EMA considers **at least** the following **firm-facing requirements should remain in legislation**:

- **Core regulatory perimeter:** including regulated e-money and payment services, core definitions and well as exclusions and territorial scope of the UK's payment services authorisations regime;
- **Small institution exemption regime** from full authorisation requirement: as this is a perimeter question in substance, and both existing and entrant firms need certainty over regulatory parameters of the regime;
- **Agent and distributor rules:** the provisions enabling payment services to be provided through agents, as well as distribution and redemption of e-money through distributors, since in essence these are regulatory perimeter defining provisions;
- **Core authorisation conditions and requirements:** e-money and payments firms need predictability and continuity in the conditions they need to meet to be authorised, and this applies to both new entrants planning for authorisation and already authorised firms;
- **Core safeguarding regime and insolvency protections:** safeguarding rules in the PSRs and EMRs set the legal features of the safeguarding regime and its interaction with priority rights over the safeguarded funds on a firm's insolvency. These provisions are supported by a body of case law that has provided important clarifications for the industry - for example, *In re Ipagoo LLP [2022]* Bus. L.R. 311 and *Re Allied Wallet Ltd [2022]* EWHC 1877, where the courts have confirmed that safeguarding provisions in the EMRs and the PSRs do not create a statutory trust for customers. The EMA therefore considers there is a case for retaining **the core safeguarding provisions in legislation, to preserve legal certainty and continuity, and to ensure that the legal principles established by case law continue to be relevant after the MPR reforms are implemented.**
- **Core provisions preserving Open Banking rights of access, including the new right of access supporting variable recurring payments:** as more fully discussed in response to **Q26**.

Question 2: Where you believe requirements should remain in legislation, are there any updates you believe need to be made to these requirements?

As outlined above, we welcome HM Treasury's overall guiding objective for balanced delegation of firm-facing rules to the FCA where this brings genuine flexibility and a more agile, outcomes-focused approach, alongside the retention of essential provisions in legislation to preserve certainty and predictability for firms. That said, the EMA believes that **the current PSRs/EMRs framework has, overall, worked successfully** - fostering innovation, competition and growth in UK payments and e-money sector - and that **any change, whether delegated to the FCA or amended within retained legislation, should only be pursued where there is a clear, demonstrable benefit**. Poorly targeted regulatory changes unavoidably introduce costs and divert firm resources, which may undermine the very objectives the MPR reforms are intended to achieve.

Against this background, whether the requirements are retained in legislation, or delegated to the FCA, the EMA advocates for change or improvement in the areas outlined in the Table below.

In addition, we address **Open Banking related updates**, including perimeter-related definitions (AIS, PIS, “accessible online”, “sensitive payment data”) in response to **Q25** and more generally the regulatory framework updates in response to **Q27**.

Topic/ Update	Explanation and recommendation
Safeguarding with the Bank of England	As set out in the Payments Forward Plan, the Bank of England's work programme already underway is to consider offering overnight safeguarding facilities to FCA-authorised Non-Bank Payment Service Providers (NBPSs), including EMLs and PIs, that hold a RealTime Gross Settlement (RTGS) settlement account. The industry strongly supports, has long advocated for, and would like to see acceleration of the Bank of England's work programme to enable the use of RTGS settlement accounts for safeguarding. The industry would also like to see the Bank to widen access to remunerated central bank account facilities, including for firms without direct RTGS participation. Allowing EMLs and PIs to safeguard directly with the Bank of England would remove systemic/concentration risks in the small pool of banks currently willing to hold safeguarding accounts, operational risks associated with back and forth movements between RTGS settlement accounts and safeguarding bank accounts, strengthen consumer protection, and help resolve the de-risking challenges facing the sector. It would also enable EMLs to compete on a more level-

Topic/ Update	Explanation and recommendation
	playing field with banks, especially if EMIs and PIs were allowed access to the BoE's interest rate on safeguarded funds. Fundamentally, this is an issue of enabling growth and innovation by levelling the playing field between commercial banks and NBPSPs. Credit institutions can place funds with the Bank of England and earn bank rate, while NBPSPs safeguarding economically equivalent funds cannot on a near equal basis, and a genuine level playing field requires access to central bank money on more equivalent, remunerated terms.
Bank account access (Regulation 105 PSR)	For a regulatory environment to support innovation, competition and growth, it is no longer acceptable that authorised firms are denied access to banking services fundamental to their business, based on the commercial or risk-appetite-based decisions of their banking partners. Based on the evidence from the EMA members, bank due diligence processes for opening an account are especially burdensome and take 6-12 months to complete. There is also a very limited number of UK banks which offer banking facilities to non-bank PSPs. Many of the EMA members have been impacted by bank de-risking, with their accounts closed with little to no notice, finding themselves scrambling to secure and migrate to alternative banking facilities. Plainly, the current situation is not conducive to competition nor consumer protection or confidence in non-bank PSP services. Despite the the requirement for proportionate, objective and non-discriminatory access to banking services for EMIs and PIs since implementation of PSD2 in 2017, nearly 10 years later the de-risking problem persists, creating barriers to entry for new market entrants, distorting the competitive landscape in favour of legacy banks, and creating a concentration risk of several accounts held with few credit institutions. This is a cross-sectoral issue that affects not only non-bank PSPs, but also cryptoasset service providers, and requires ever more urgent, co-ordinated policy resolution if the UK is to achieve its ambition of becoming world leader in tokenised payments. EMA recommends: • Make account access a right for non-bank PSPs, with the FCA mandated to intervene where access is not forthcoming; • Banks should be subject to a higher duty when justifying the refusal to offer account services to PSPs, as distinct from other

Topic/ Update	Explanation and recommendation
	businesses, and this should not be solely a commercial or risk-appetite-based matter; • Mandated process and timelines account application and refusal decisions by banks; we suggest 1 month for a bank to provide a decision on account application submission, and minimum 6 month account termination notice with a standstill until a replacement account is secured; • FCA should publish data on the number of PSPs that are de-risked or refused an account at the application stage, providing transparency and accountability on the issue. The EU's forthcoming Payment Services Regulation mandates similar improvements through its bank account access provisions; our proposed approach above should enable alignment with the EU PSD3/PSR reforms and more level playing field for UK PSPs when compared with their EU counterparts. An alternative or additional approach might be for the government to set up an entity whose purpose is to provide safeguarding and other bank accounts to entities within the Fintech sector for whom access to a bank account represents a significant barrier to doing business - like the British Business Bank for example.
Prohibition of interest rule (Regulation 45 EMR)	The EMA recommends that the prohibition on EMIs awarding interest, or other benefits related to the length of time e-money is held in Regulation 45 of the EMRs is reassessed with a view to removal, for the following reasons: • The original rationale no longer reflects the market: The rule derives from the EU's second Electronic Money Directive set in 2009, which treated e-money as "an electronic surrogate for coins and banknotes ... usually of limited amount and not as means of saving". Nevertheless, it no longer reflects the market, where the e-money based products have evolved and cover a broad range of propositions. For example, EMIs can offer current-account-style accounts into which salaries are paid, business and treasury accounts, multi-currency accounts. No limits apply to the amounts that may be held, and many customers keep significant balances for extended periods for entirely legitimate payment purposes. Customer expectations have changed accordingly: users increasingly expect the funds they hold to generate value or some other form of benefits or rewards, whether those funds are held as deposits, e-money or

Topic/ Update	Explanation and recommendation
	in other financial products, irrespective of their legal form. • Distorts competition and prevents sharing returns with customers: The prohibition puts EMIs at a structural disadvantage to banks, which compete for the same customers and use cases but are free to pay interest. It prevents EMIs from sharing the interest earned on the safeguarded funds or other time-linked benefits with their customers. Allowing EMIs to pass on those returns would support the Government's competition objective and improve ability to deliver fair value for customers, in line with the Consumer Duty. • Prudential risks already addressed: Any underlying concerns, such as that e-money issuers should not become deposit-takers, is already addressed more directly by other requirements: safeguarding, redemption at par and the prohibition on granting credit from funds received in exchange for e-money. Passing on returns actually earned on safeguarded funds or assets involves no lending or maturity transformation and does not change the protected status of customer funds. Paying interest therefore should not amount to nor imply the same risks as deposit taking activity. The EMA considers this is also the right moment to reassess the question in the context of the UK's future regime for stablecoins. Whilst the FCA's final rules (as confirmed in PS26/10) prohibit issuers of qualifying stablecoins from paying interest or income from the backing asset pool to tokenholders, the FCA has committed to further work exploring "the competition and economic implications of offering interest". As e-money and stablecoins will be increasingly used for the same payment purposes, and, as this consultation proposes, tokenised payments will sit within the payments framework, the Government should therefore consider the treatment of interest across both regimes together, on the basis of evidence about risks and outcomes. Otherwise, there is a risk a prohibition inherited from EU law could be locked into both regimes without appropriate, evidence based justification.
FCA's discretion over own funds (Para. 4 of Schedule 3 to the PSR; Para. 15 of Schedule 2 to the EMR)	The FCA can direct the own funds calculation method to be used or that the amount of the own funds is to be up to 20% higher than the resulting calculation. This can result in uncertainty over the own funds requirements at the authorisation application stage. There is a tendency to err on the side of caution, resulting in onerous obligations that may deprive a business of working capital without contributing significantly to risk mitigation. Operational risk may not necessarily be addressed by increasing own funds requirements.

Topic/ Update	Explanation and recommendation
	EMA recommends: • Set better defined and consistent criteria (in legislation or secondary guidance) for the FCA's approach, that is proportionate to the operational and financial risks faced by payment firms; and • Any additional capital buffer (up to the current 20% uplift) should be time-limited and automatically reassessed for release, to ensure that capital resources are not tied in unnecessarily.
Safeguarding by investments (Regulation 21(6)(b) PSRs; Regulation 23(6)(b) PSRs)	A reasonable expansion of the range of eligible assets EMIs and PIs can invest in would support economic growth and consumer benefit, by giving firms a genuine opportunity to generate a return on safeguarded funds that can be reinvested in better-priced, more innovative products. EMA recommends: • The assets that EMIs and PIs can invest in should be widened to those that are of a high quality but less liquid, at least for that part of safeguarded funds that is not likely to be required to meet redemption requests at short notice; and the FCA's guidance on what assets qualify currently should be improved in the interim. • The mandatory requirement for a custodian to hold assets firms invest in should be revised - it blocks firms from investing directly in vehicles like money market funds, adding counterparty risk and cost without any corresponding safeguarding benefit.
App Scam Reimbursement Requirement	Review the full reimbursement policy, including the scope of transactions and types of fraud (scams) that are in scope. The scope of the policy is too wide and far too complex for customer contact staff to handle claims correctly, and must be simplified. EMA recommends: • Amending the liability on Sending PSP and Receiving PSP to 75/25% (max £25k) for loss arising from an APP scam to better reflect the prudential risk borne by smaller Fintech Receiving PSPs. • Removing from scope purchase scams, as these are high volume, low value, and a high risk of being a buyer seller dispute rather than a genuine scam. There is a high proportion of invalid claims (20%+) that require a disproportionate amount of PSP resources to process. • The PSR's fraud originations report published December 2024, using data from the 14 largest UK bank PSPs identifies the

Topic/ Update	Explanation and recommendation
	significant role social media and tech platforms play in the recruitment of APP Scam victims. As such, they must be enlisted to play their role in assisting PSPs in the fight against fraud. ● Reviewing the Consumer Standard of Caution, including: ○ mandating customers to lodge a crime report with the police in order to qualify for the full reimbursement of a fraudulent transaction under the APP Scam reimbursement, and ○ rebalancing the responsibility placed on a consumer when pursuing high value ‘investment’ transactions.
Payer’s liability threshold (unauthorised transactions) (Regulation 77(1))	The EMA considers the maximum liability amount the payer can be held responsible for in relation to unauthorised transactions as set out in this regulation should be increased. EMA recommendation: We consider an increase to £100 to be reasonable. This increase would reflect inflation as well as discourage carelessness or reckless behaviour by payers, in looking after their payment instruments or the security credentials used to access them.
Strong Customer Authentication (Regulation 100 PSRs; UK Regulatory Technical Standards on SCA)	Consultation confirms the government’s commitment to revoke the payment’s authentication regulations relating to Strong Customer Authentication (SCA) in the PSRs to enable the FCA to make more outcomes-based rules about authentication requirements. The EMA has a number of recommendations to table in that regard, including: ● Enable application of more flexible, risk-based customer authentication techniques (e.g. leveraging a single authentication element type) for lower-risk interactions; ● Expressly narrow the scope of SCA-triggers interactions to: ○ high risk payment service user interactions with a payment account accessible online (directly or via a TPP); and ○ electronic payment transactions initiated by the payer (with dynamic linking requirement retained in this instance). ● Allow greater flexibility in (or an exemption from) the application of SCA to corporate users, whose interactions with PSPs carry a lower risk profile and often already benefit from embedded security controls. This is set out further in relation to the <i>corporate opt out</i> point below. The EMA believes these recommendations would maintain the existing high levels of security that SCA is designed to meet, whilst at the same

Topic/ Update	Explanation and recommendation
	time improving efficiencies, and moving towards a more risk- and evidence-based approach. Additional recommendations on the SCA exemptions and authentication elements are set out in the EMA's submission to the FCA in March 2024.
Low value payment instrument thresholds (Regulation 42 and 65 PSR)	The current value limits for low-value payment instruments are too low, meaning that PSPs are seldom able to utilise the simplified frameworks provided for under regulations 42 and 65. EMA recommendation: increase the low value instrument threshold values to reflect inflation and utility of instruments. We consider an increase in value to EUR 100 for individual transactions, and spending and storage limits to EUR 500 would be reasonable. Note that an increase in thresholds also aligns closer with the EU's PSD3/PSR thresholds, where both the storage and spending limits will increase to EUR 300 or EUR 500 for prepaid payment instruments.
Limited Network Exclusion (LNE) (Paragraph 2(k) of Schedule 1 to the PSRs; Regulation 38 PSRs; Regulations 3(a) and 3A EMRs)	The Limited Network Exclusion (LNE) exempts from the e-money and payment services regulatory framework simple, restricted use instruments such as gift cards. To be clear, LNE continues to be valuable to ensure a proportionate regime for the products it covers, and should be retained in the future framework. Nevertheless, there are two distinct issues which may warrant revision. Scope: PSD2 narrowed LNE to instruments usable only in a "limited way" but this leaves out payment instruments whose acceptance is restricted in practice yet don't meet the technical LNE test. Issuers of these products must obtain full EMI authorisation, a disproportionate burden for products that function much like excluded ones (e.g. gift cards) and were never intended to compete with unrestricted e-money. The LNE conditions should be revisited against actual market practice and consumer usage/expectations. Notification process (Reg 38 PSRs): the current regime is administratively burdensome and creates uncertainty. • Notification is only triggered after transaction volumes exceed €1m in a 12-month period, forcing reactive rather than up-front notification. The EMA recommends an allowance for up-front notification should also be made to avoid the service providers having to terminate products, if the FCA takes a view the product does not meet the LNE conditions. We also suggest that the threshold trigger for notification should be increased

Topic/ Update	Explanation and recommendation
	(from EUR 1 million) to EUR 3 million to address increased use of non-cash products and inflation. • The FCA has no deadline to respond on LNE notifications. The FCA should be required to respond to the LNE notification with any objections it may have within a timeframe specified in statute (we suggest a timeframe of 2 months), and if the FCA does not respond within this period, it should be deemed to have agreed to the service provider's notification. This would reduce uncertainty faced by service providers following the submission of LNE notification. • Firms must currently re-submit their LNE notifications annually, creating unnecessary administrative burden. Re-notification should be limited to instances involving <i>material</i> changes to the initial submission only (e.g. a new LNE product range, not a new merchant joining an existing network), which would make it consistent with the EU approach. As a further alternative, the notification requirement could be removed altogether, given its likely limited supervisory value, and aligning with the EU's PSD3/PSR approach which makes notification requirements optional at Member State discretion. In any case, we suggest it would be helpful to maintain informal regulatory consultation channels with the FCA, so that regulatory classification of prospective LNE product propositions, for example in less straightforward cases, can be discussed with the FCA as needed.
Electronic Communications Exclusion (ECE) (Paragraph 2(l) of Schedule 1 to the PSRs; Regulation 39 PSRs; Regulations 3(b) and 3B EMRs)	The Electronic Communications Exclusion (ECE) exempts from the e-money and payment services regulatory framework certain payment transactions made through, for example, a mobile network operator, and charged to the subscriber's bill. It covers purchases of digital content and voice-based services (such as apps, games, music), as well as electronic tickets and charitable donations made from or via an electronic device. ECE allows low-value, convenient "carrier billing" services to be offered, without that provider having to be authorised; it remains valuable and should be retained under the future framework. Nevertheless, the monetary limits for the ECE set in the regulations (£40 per transaction and £240 cumulative per subscriber per month) were set when PSD2 was transposed in 2017 and have not been revised since. They no longer reflect inflation or the prices of the digital content, ticketing and charitable giving the exclusion is meant to cover. As a result, the exclusion's practical value has fallen over time, and operators may move outside its perimeter for reasons unrelated to the risks of the activity.

Topic/ Update	Explanation and recommendation
	The EMA recommends: • ECE limits should be increased, to the levels that restore the practical utility of the exclusion and enable meaningful purchases of digital content, tickets and other services that the exclusion is intended to cover. In determining the appropriate thresholds, HMT Treasury should take account of inflation since the existing limits were introduced, as well as changes in the prices of the relevant goods and services. We suggest that, at a minimum, the revised UK thresholds should not be lower than £60 per transaction and £360 per month, reflecting broad parity with the EU's PSD3/PSR increased limits for ECE (EUR 60 and EUR 360 respectively), with a further uplift considered to reflect UK inflation since 2017 and the evolving cost of goods and services the exclusion is intended to cover; • In addition, we invite HMT to consider whether the mandatory notification and annual audit opinion regime for ECE under regulation 39 PSRs remain proportionate, given that they carry administrative burdens yet are likely of limited supervisory value for the FCA. Removal of these requirements would also align with the EU's PSD3/PSR approach, where the notification requirements become a Member State option.
Monetary thresholds and inflation	As highlighted above, a number of exclusions and other provisions of the PSRs and EMRs contain monetary thresholds dating from PSD2 or earlier. These thresholds were set more than a decade ago and do not reflect inflation. In addition to our specific suggestions above to update the thresholds, the EMA believes the regulatory framework would benefit from a more general mechanism for reviewing thresholds periodically to take account of inflation. In keeping with HM Treasury's broader objectives of an agile, and future-proofed regulatory framework, this would enable keeping thresholds relevant over time without waiting for legislative or other regulatory reforms. We note such an update mechanism would also mirror the EU's PSD3 and PSR, whereby the EU Commission is empowered to update, inter alia, the small-institution exemption thresholds and the cap on payer liability for unauthorised transactions. It is not suggested, however, that the UK's inflationary updates should be reserved for these provisions covered by the equivalent EU mechanisms only; updates may be equally necessary in respect of other monetary thresholds, such as the notification threshold for the limited network exclusion (LNE) and the transaction limits for the electronic communications exclusion (ECE)

Topic/ Update	Explanation and recommendation
	noted above. EMA recommendation: The EMA suggests that the relevant monetary thresholds in the PSRs and EMRs should be made subject to periodic review (for example, every five years) against an appropriate inflation index, with HM Treasury (or the FCA, where thresholds are delegated to rules) under a duty to consider updating them.
Corporate opt-out (Regulation 40(7) and 63(5) PSR)	The PSRs already recognise that customers who are not consumers, micro-enterprises or small charities do not need the same level of protection, and allow them to agree with their PSP to disapply the information requirements in Part 6 and a defined list of rights and obligations in Part 7 of PSRs. Corporate opt out regime has proven effective in achieving proportionality and supports the core English law principle that commercial parties should be free to agree terms suited for their relationship. <u>The EMA strongly supports preserving the corporate opt-out provisions under the future framework.</u> That said, the list of Part 7 provisions subject to a corporate opt-out remains largely unchanged since PSD2. EMA considers that there is a case to expand it, so that PSPs and their larger corporate customers can agree to disapply certain further requirements where these are not suited to the corporate relationship. Corporate customers often have dedicated treasury and finance functions, negotiate bespoke contractual terms and security controls, and are well placed to judge which protections they need and which they would rather replace with arrangements tailored to their own operations. In particular, the EMA recommends to expand the scope of the corporate opt out in respect of the following: • Strong Customer Authentication. As noted in the EMA's submission to the FCA in March 2024, the user-service interactions that involve corporate users often benefit from additional security controls compared to the interactions that involve individual users and the lower overall risk associated with corporate users' interactions with PSPs. Article 17 of the UK's SCA Regulatory Technical Standards (RTS) enables an exemption for secure corporate payment initiation, but the current regulations still trigger SCA requirements for other corporate user interactions (such as account logins to view or run reports, revise customer contact details etc.). The requirement to implement SCA using authentication elements/factors that are suited for retail customer use cases where the user is actively present in the service access flow (e.g. entering passwords or

Topic/ Update	Explanation and recommendation
	OTPs, completing biometric authentication on a customer device) introduces additional complexity and unnecessary friction to automated corporate payment service APIs or to web-based access portals. Such service access channels already benefit from the deployment of embedded security controls that offer equivalent levels of security as retail payment service access channels that enforce mainstream SCA requirements. In this context, we propose that PSPs are afforded more flexibility in the application of SCA for service access interactions involving corporate users. For example, this flexibility could be achieved through expansion of the Article 17 of UK SCA RTS to cover <i>the entirety</i> of SCA-triggering interactions that involve corporate users (<i>i.e. accessing a payment account, initiating payment, actions carried out through a remote channel that give rise to a fraud risk</i>). ● Refund and liability provisions. The corporate opt-out already applies to certain PSP liability and refund provisions. However, its usefulness may be decreasing as the payment services regime evolves or new liability requirements are introduced. For corporate customers, the allocation of liability and risk is ordinarily a commercial matter, reflected in pricing, insurance and the customer's own controls. The EMA would therefore welcome HM Treasury keeping under review whether any refund on liability related requirements should be open to agreement between the parties for corporate customers, particularly as new liability frameworks develop, for example for new payment models.

Question 3: Do current provisions relating to the regulatory framework for payment services and electronic money, such as key definitions, need to be updated? If so, please explain how.

Definition of “funds”

The current definition of “funds” in regulation 2(1) PSRs covers banknotes and coins, scriptural money and electronic money. To ensure that the future regime covers both fiat and tokenised payment activities, the definition of “funds” will need updating to encompass stablecoins and tokenised deposits.

Definition of a “payment account”

The definition of "payment account" in regulation 2(1) PSRs is: "an account held in the name of one or more payment service users which is used for the execution of payment transactions." The legal definition is broad, technologically neutral and capable of capturing a broad range of account arrangements, whilst remaining of key interpretative importance, because it determines which accounts are subject to the TPP access obligations (regulations 69–70). In practice, its scope is currently informed by case law and regulatory guidance. For instance, following the CJEU's judgment in *ING-DiBa* (C-191/17), FCA guidance at PERG 15.3 (Q16) suggests the ability to make payment transactions to, or receive them from, a third party as one of the defining features of a payment account. The EU's PSD3/PSR definition has moved to explicitly clarify that a payment account must enable both sending *and* receiving of funds. The EMA is supportive of this qualifying criterion, as it has proven to be pragmatic in practice, noting it is possible to suggest that other functionalities can also distinguish payment accounts. Nevertheless, the EMA believes it may be helpful for the definition of payment accounts to be clarified within PSRs itself, and for this to be set out in a pragmatic manner. The scope of accounts that are captured is still subject to difference of interpretation, with resulting uncertainty over which accounts are available to PIS and AIS providers.

Even within a clearly defined scope of "payment accounts", we note that some payment accounts attract little or no demand from TPPs, and the ASPSP obligation to build and maintain dedicated access interfaces for them may be disproportionate. The definition should therefore be read together with our proposal at Q27 for a demand-based exemption from the requirement to provide access interfaces. Taken together, these should ensure a proportionate approach where access obligations apply to the accounts where TPP access delivers real value for users.

Open Banking

We address additional Open Banking-related updates, including perimeter-related definitions (AIS, PIS, "accessible online", "sensitive payment data") in response to **Q25** and more generally the regulatory framework updates in response to **Q27**.

Question 4: Which international regulatory developments, for example recent reforms in the EU, should the UK incorporate into an updated framework for payment services and electronic money?

EU's PSD3 / PSR

Many of EMA members operate across both the UK and EU, and - generally speaking - value consistency in regulatory standards, given the benefits of interoperability and shared compliance burden across their group operations. The EMA supports monitoring, and - where appropriate and beneficial for the UK payments framework - incorporating developments from the EU's PSD3/PSR package. The EMA has identified specific areas of potential PSD3/ PSR alignment throughout this response document, in particular in response to: Q2, Q3, Q9, Q17, Q22, Q26, Q27.

SEPA Continuity

UK's continued membership of the Single European Payment Area (SEPA) ensures efficient, low-cost euro payments for UK consumers and businesses, and preserves interoperability with the EU's dominant retail euro payments infrastructure, all of which are of direct importance for competitiveness of the UK payment services sector.

The EMA urges the government to treat continued UK participation in SEPA as a strategic objective of the reformed payment services framework. Because SEPA access turns on UK regime's substantial equivalence with PSD2 (and future PSD3/PSR) standards, the EMA believes the government's MPR programme would benefit from a dedicated assessment specifically which elements of the new EU PSD3/PSR package the UK's reformed framework would need to incorporate in order to preserve equivalence for SEPA purposes.

Question 5: Does the current regulatory framework need to adapt to unlock the opportunities arising from the use of tokenised deposits in retail payments?

We do not consider that significant changes to the existing regulatory framework are required. The government's priority should be to ensure that the framework clearly recognises tokenised money as funds and applies the same regulatory requirements irrespective of the technology used.

Tokenised deposits are already recognised as deposits pursuant to FSMA; the focus should therefore be on ensuring clarity and consistency between the payments and cryptoassets regulatory regimes, so that the use of tokenised deposits for payments does not create unnecessary regulatory overlap, duplication or uncertainty.

We support the government's proposed principle of "same risk, same regulatory outcome" and consider that any changes should be limited to those necessary to provide this clarity.

Question 6: Do you agree that only stablecoins issued in the UK or from a recognised jurisdiction should be treated as money-like for the purposes of payments, and brought into the UK payments perimeter?

We broadly agree with the proposed approach. Stablecoins should only be treated as money-like for the purposes of payments where they are subject to an appropriate regulatory framework that provides sufficient confidence in their stability and backing.

It will, however, be important for the recognition framework for overseas jurisdictions to be clear and proportionate. Firms need certainty as to which stablecoins can be treated as money-like and brought within the payments perimeter, and which remain subject to the cryptoassets regime. I.e. there would need to be official recognition similar to adequacy decisions for GDPR.

Recognition of stablecoins issued in appropriately regulated overseas jurisdictions could provide real benefits for UK payment firms, particularly in relation to cross-border payments. Stablecoins have the potential to support faster settlement and reduce some of the cost and complexity associated with cross-border payments. Recognition would also allow UK firms to use stablecoins issued in other well-regulated markets, rather than limiting the development of these services to UK-issued stablecoins.

We would expect the government to consider jurisdictions such as the EU, where MiCA establishes a regulatory framework for stablecoin issuance, including requirements relating to authorisation, reserves and redemption. Other jurisdictions with established regulatory regimes for fiat-referenced stablecoins, such as Hong Kong and the US perhaps, should also be considered for recognition.

Question 7: Should firms authorised to issue UK-issued qualifying stablecoins be allowed to provide payment services without additional permissions, but be subject to relevant requirements?

Yes, permitting the UK-authorized stablecoin issuer may only provide payment services in relation to stablecoins and not payment services in general i.e. in fiat.

Question 8: Do you agree that safeguarding of UK-issued qualifying stablecoins, where that is within new article 9M RAO, for the purposes of payments should eventually be regulated under the payments regime and not the cryptoassets regime?

The EMA wrote a letter to HMT on this point following the roundtable between HMT and the EMA on Tuesday 29 September 2026. The letter is reproduced below for reference:

I write to follow up on the roundtable meeting that took place between HMT and the EMA on Tuesday 29 September 2026 in relation to the above consultation. The meeting was only scheduled for one hour and we therefore did not get a chance to discuss several important issues, including tokenised payments. You asked me to follow up with you in writing.

The issue I wished to raise with you on the day of the roundtable was a specific issue concerning the regulatory treatment of stablecoins when they are used for the provision of payment services, and in

particular the requirements that would apply where a payment service provider (“PSP”) holds and safeguards stablecoins on behalf of its customers.

We welcome the decision to exclude from the UK financial services regulatory framework for crypto assets the regulated activities of dealing in qualifying cryptoassets as principal, dealing as agent, and arranging deals in qualifying cryptoassets when these activities are carried out in relation to UK qualifying stablecoins.¹ These exclusions create a significant opportunity for payment firms to develop new products and services that allow customers to make and receive payments using stablecoins alongside traditional fiat funds.

There is, however, a risk that this opportunity will be disproportionately constrained by safeguarding requirements. Whilst dealing and arranging have been excluded from the scope of the cryptoassets regime in these circumstances, a PSP wishing to hold stablecoins for customers would, generally speaking, still need to obtain a Part 4A permission in respect of safeguarding those stablecoins.²

We recognise the temporary settlement arrangements introduced through new Articles 9Q and 9QA of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (S.I. 2001/544) (“RAO”) under the recently laid Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026. These exclusions are helpful where a PSP holds stablecoins only temporarily as part of the execution or settlement of a payment transaction. However, the exclusions are expressly limited to “temporary” holding arrangements and which the FCA has recently indicated they interpret “temporary” to mean a period of 24 hours or less.³

They therefore do not address the position of PSPs that wish to hold stablecoins for customers for longer periods, including where a PSP wishes to provide a wallet, stored-value functionality or another payment product under which stablecoins remain available to the customer pending their subsequent use for transacting.

We do not consider that requiring PSPs to obtain a Part 4A permission solely for this purpose would be proportionate. Safeguarding is a regulatory obligation for payment and e-money institutions. Firms do not regard safeguarding as a separate commercial activity or privilege; it is an obligation imposed

¹ Pursuant to the draft Financial Services and Markets Act 2000 (Cryptoassets) (Miscellaneous Amendments) Regulations 2026

² Pursuant to Article 9N of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (S.I. 2001/544)

³ See incoming PERG 18.6.6 set out in Policy Statement PS26/18: PERG 18.6.6 “ [...] ‘Temporarily’ is also undefined but is likely to mean that the safeguarding lasts only as long as necessary to facilitate settlement. In practice, the FCA considers that this is unlikely to require longer than 24 hours from the point at which the requisite degree of control exists [...]”.

upon them precisely because they hold customer funds in connection with the payment services they provide.

Requiring an otherwise appropriately authorised PSP to obtain an additional Part 4A permission because the customer assets being safeguarded are stablecoins rather than fiat funds would therefore create a significant additional regulatory burden. In practice, we are concerned that many PSPs would decide that the cost and complexity of obtaining and maintaining the additional permission makes offering stablecoin payment services commercially unattractive.

We would therefore welcome the opportunity to explore an alternative approach with HM Treasury that provides equivalent protections for customer stablecoins without requiring PSPs to obtain a separate Part 4A safeguarding permission.

One possible approach would be to apply the substantive requirements of CASS 17 to PSPs that safeguard stablecoins in connection with regulated payment services. PSPs would therefore be required to comply with the same safeguarding standards applicable to cryptoasset firms holding qualifying cryptoassets for clients, without the safeguarding activity itself triggering a separate Part 4A authorisation requirement.

Our preference, however, would be to consider an approach more closely aligned with the existing payments safeguarding framework. This could, for example, require stablecoins held by a PSP to be segregated from the firm's own assets and appropriately protected for the benefit of customers. Such an approach could draw on the principles in CASS 15 whilst reflecting the existing safeguarding arrangements with which PSPs are already familiar.

The objective should be to achieve the appropriate safeguarding outcome without unnecessarily requiring payment firms to enter a separate authorisation regime merely because they wish to add stablecoins to their existing payment products.

We consider there is a genuine opportunity for the UK payments sector to develop innovative stablecoin-based payment products and services. It would be unfortunate if the benefits of the decision to facilitate stablecoin payments through the payments regulatory framework were substantially diminished by a separate authorisation requirement arising solely from the need to safeguard the stablecoins used in providing those services.

We would therefore welcome further engagement with HM Treasury on how an appropriate safeguarding framework can be developed that provides protection for customers while allowing PSPs to take advantage of this opportunity in a proportionate and commercially viable manner.

Question 9: Do you agree with the proposed broad split of regulated activities for payments and electronic money issuance?

Yes, the EMA does not object to the government's proposed broad split of regulated activities for payments and electronic money issuance.

We note that the proposed list reflects the revised payment services list under the EU's PSD3, which for firms operating under both UK and EU frameworks may support consistency in their regulatory permissions and how these translate operationally across their UK and EU businesses.

That said, the EMA raises the following points on the specific proposed changes:

- **Issuance of electronic money:** The EMA strongly supports the Government's proposal to retain e-money issuance as a distinct regulated activity within the framework.
- **Cash placement/withdrawal activity:** The EMA queries whether "and all operations required for operating a payment account" should remain part of the scope of this specific (now-merged) activity in its current formulation. Cash placement/withdrawal from a payment account the PSP operates is a regulated activity; however, operating a payment account should not, in and of itself, constitute a regulated activity. Nevertheless, in practice this reference to payment accounts has at times led to the suggestion that a firm requires this permission even where it offers no cash placement or withdrawal services at all, simply because it operates a payment account. This approach could create an unnecessary duplication with other activities, such as "execution of payment transactions" activity, which already captures payment account transaction related activities more generally. The EMA would welcome clarification of this qualifying language in relation to the cash placement/withdrawal activity specifically, so that firms are not required to hold two overlapping permissions for the same underlying activity.

In addition, we have the following points to raise on the future transitioning to the MPR's new payment services and e-money activities regime:

- **Seamless transition of existing permissions.** Ensuring seamless transition of existing permissions to the new activity structure is one of the EMA membership's top priorities in respect of these MPR reforms. The EMA asks the Government to clarify how authorised firms' existing permissions would be transitioned, and to ensure that any transition is made seamless for existing firms - for example, through a deemed permissions approach that maps current permissions automatically onto the new activities. The EMA would be strongly opposed to any requirement for re-authorisation, which principally amounts to a paper exercise that is a significant drain on firm resources without any corresponding regulatory benefit, when resources could otherwise be invested in innovation or growth generating activities.

- **E-money issuers providing payment services in e-money.** The EMA supports retaining the current approach whereby e-money issuers (electronic money institutions) can provide payment services without needing to seek separate permissions.
- **Level-playing field for gaining AIS/PIS permissions.** EMLs and PIs need additional approval of variation of permissions applications to provide AIS and PIS services, whereas credit institutions only need to notify the FCA. The EMA supports equalising the approach for all institutions, to avoid competitive advantages gained by credit institutions under the current approach (see further our response to Q27).

Question 10: Do you agree with the proposal to have a single set of regulated payments activities for both tokenised and non-tokenised payments? Are there any risks associated with combining activities in this way? If so, should these risks be mitigated by framing regulated payment services activities differently?

Yes. We agree with the proposal to have a single set of regulated payment activities for tokenised and non-tokenised payments.

We do not consider that a separate set of regulated activities is needed simply because the funds used to make a payment are tokenised. The payment activity remains the same whether the payment is made using fiat funds, e-money, a qualifying stablecoin or a tokenised deposit. The regulatory framework should therefore focus on the nature of the payment service being provided rather than the technology or form of the funds used to provide it.

This is also consistent with the government's proposal that the payment activities currently contained in Schedule 1 to the PSRs should broadly form the basis of the new regulated activities, with those activities capable of being carried out using both fiat and tokenised payments. We agree that this is preferable to creating separate permissions for fiat and tokenised versions of essentially the same payment service. As the consultation recognises, separate permissions would also create additional administrative burdens for firms providing integrated fiat and stablecoin payment services.

Question 11: Do you agree that authorised and registered firms should require a variation of permission to carry out payment services using tokenised payments?

Yes, provided that the variation of permission process is implemented by the FCA in a reasonable and proportionate manner.

We recognise the FCA's need to understand the activities being undertaken by firms within its payments portfolio, particularly where a firm proposes to introduce a new product or a material

change to its business model. Firms already engage with the FCA in these circumstances, and we therefore accept that there is a role for a variation of permission where a firm proposes to provide payment services using tokenised payments.

We would, however, have concerns if this were implemented by imposing a general restriction on payment institutions from the outset which prevents them from providing payment services using stablecoins unless and until that restriction is subsequently removed.

We have seen the FCA make increasing use of restrictions at the authorisation gateway under which firms are asked to agree that they will not undertake particular activities. For example, firms may be required to undertake not to use e-money distributors, or a firm with a B2B business model may be restricted from providing services to consumers. The firm must then apply for a variation of permission if it subsequently wishes to undertake the restricted activity.

We would not support the same approach being applied generally to tokenised payments. The government's proposal is for the same regulated payment activities to apply to both fiat and tokenised payments. It would undermine that approach if all PSPs were effectively subject from the outset to a restriction preventing them from providing those services using stablecoins.

We therefore agree that a variation of permission can provide an appropriate mechanism for the FCA to be notified of, and consider, a firm's proposed use of tokenised payments. However, the process should be proportionate to the change in the firm's activities. Nor should it be implemented through a general presumption that existing PSPs are prohibited from providing payment services using stablecoins.

Provided the FCA operates the variation process fairly and proportionately, and does not use it to impose a general restriction on stablecoin payment activities from day one, we agree with the proposal.

Question 12: How does the payment services regulatory framework need to adapt to support the use of smart contracts and programmable payments underpinning them?

We do not consider that the payment services regulatory framework needs to be adapted specifically for smart contracts or programmable payments. Smart contracts are a use case for making payments, rather than a separate payment service.

The regulatory framework should remain technology neutral and apply to the underlying payment activity irrespective of the technology used to initiate or execute the payment. Where clarification is needed as to how particular requirements apply to smart contracts or programmable payments, this

could be addressed through FCA guidance e.g. Approach Doc or ad hoc guidance, rather than changing law or regulation.

Question 13: Are the current conduct of business requirements in the payment services regulatory framework suitable for tokenised payments? Please explain your answer.

Yes. We consider that the current conduct of business requirements are generally suitable for tokenised payments.

The conduct requirements should remain technology neutral and apply according to the payment service being provided, rather than the form of the funds used to make the payment. We do not consider that the use of stablecoins, tokenised deposits or other tokenised forms of payment requires a separate set of conduct requirements. This is consistent with the Government's broader approach of considering whether tokenisation creates risks which are not already addressed by the existing framework.

In particular, we do not consider that separate information or liability requirements are needed simply because a payment is tokenised. The Consumer Duty already requires firms to focus on the outcomes received by retail customers. Compliance cannot therefore be approached solely by prescribing additional wording for framework contracts, notifications, warnings or other customer-facing documents. PSPs must consider whether the information and support they provide enable customers to understand the service and whether the overall product delivers good outcomes.

Anything additional the FCA wish to impose can be addressed in guidance, for example.

Question 14: Are the current prudential requirements in the payment services regulatory framework suitable for tokenised payments? Please explain your answer.

The principal concern is the interaction between payment service prudential requirements, COREPRU and CRYPTOPRU. COREPRU provides common prudential standards, CRYPTOPRU introduces requirements specific to regulated cryptoasset activities and COREPRU 4.1.3G expressly envisages payment institutions and electronic money institutions meeting their PSR and EMR capital requirements separately and additionally. For firms operating across both regimes this creates a risk of cumulative requirements.

Under the PSRs, authorised payment institutions generally hold the higher of initial capital and an ongoing required using one of three methods, based on overheads, payment, volumes or income.

COREPRU used a different calculation method based on fixed overheads and K- factor and had explicit liquidity and risk assessment requirements.

The interaction between these requirements must be considered, overlapping obligations identified and their cumulative application justified. A simple application of separate prudential regimes results in unnecessary financial burden for firms.

For systemic stablecoin payments, we welcome the proposed allocation of responsibilities between the Bank of England and the FCA together with the transition arrangements in the Bank of England and Financial Conduct Authority's approach to joint regulation of systemic stablecoin issuers. Moving forward clarity is needed on how the approach will extend to systemic issuers also providing payment services. The Bank of England and FCA have committed to avoiding duplication in capital, liquidity and resolution requirements. A mapping is necessary to identify which of the different prudential requirements will apply and avoid duplicate capital for the same risk within the same entity.

Question 15: How does existing payment services regulation need to adapt to support agentic payments? For example, do provisions relating to authentication and consent of payment transactions, and liability for unauthorised payment transactions, need updating?

Industry guidelines and standards ahead of modification of the PSRs

The EMA welcomes the Government's ambition for the UK to lead in agentic payments. Nevertheless, the agentic payments market and ecosystem - business models, use cases and technical protocols - are still developing, and it is not yet clear which will prevail.. Modifying the PSRs prematurely without a comprehensive understanding of these operational realities risks producing ill-fitted regulations for how the market develops and impede innovation the Government seeks to encourage. Therefore, the EMA currently advocates for an approach led by industry standards and regulatory guidance rather than legislative amendments to the PSRs. Given the rapid evolution of technology and application scenarios, modifying the PSRs now risks constraining market development. Modification of the PSRs can be implemented more effectively as market practices stabilise and mature, if the industry identifies that such modification is needed.

It should also be acknowledged that the existing regulatory framework can already be applied quite well for some agentic payments models, which to some extent depend on the role the payer plays in a transaction. For example, where the payer remains in the loop, with the agent identifying products and preparing the transaction and the payer approving and authenticating the specific payment, the existing rules on consent and SCA can in principle be applied as intended. In cases where a payment service user gives an AI agent authority to transact within defined parameters, without consenting to

each individual transaction, the payer's consent may validly be given through a mandate to an agent, as consent to a series of payment transactions within defined parameters - also a use case that the PSRs recognise.

There are also important parallels with Open Banking to be considered. For instance, the payment initiation services regime was developed in recognition that third parties able to initiate payments on behalf of customers require regulatory oversight. An AI provider that recommends a payment is very different from one that decides whether and when a payment should be made and can cause it to be initiated. Where an AI agent is acting under a continuous authority and is able to initiate payments from their account, there is a reasonable question as to whether and in what circumstances that activity may fall within the regulatory perimeter, e.g. as a PIS service. The EMA would welcome clarifications in that regard, and discuss some of the more specific Open Banking issues relating to AI in our response to Q25.

Having said that, even at this early stage of adoption of agentic payments, it is clear that to guarantee the safety and trustworthiness of the payment systems, as well as the attractiveness and innovation of the UK financial sector, a harmonisation of practices and common rules would be beneficial, particularly in the areas outlined below.

Identification of the AI Agents and AI initiated transactions

For agentic payments to be widely used and trusted across both consumers and the UK payments ecosystem, clear identity verification and transaction transparency are essential. The EMA believes two distinct requirements must become industry standards: the explicit identification of the AI agent to the customer (and their PSP), and the mandatory tagging of any transaction originating from an AI agent.

From a consumer protection perspective, rigorous agent identification is essential to ensure payment services users, and by extension its PSP, can verify the legitimacy of an agent before granting access to financial accounts or sharing payment details.

From an industry perspective, PSPs must be able to differentiate between human-initiated and AI-initiated traffic in real time. This will allow PSPs to adapt existing fraud detection models to detect and prevent emerging fraud typologies or existing typologies enhanced through AI agents. It would also permit the efficiency of Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) controls, adapted to the specificities of agentic payments, and ensure a reliable financial crime mitigation framework.

Minimum requirements for use of AI Agents (clear mandate with limited scope, record-keeping/auditability, accountability if an agent misbehaves)

To maintain user trust in UK payment systems and transactions, a set of minimum standards for AI agents should be established:

- Clear and revocable mandate: The payment service user must grant an explicit mandate that remains revocable at any point prior to payment execution. Where the scope of the mandate is not limited, the associated risks must be clearly communicated to the user, and the user's PSP should have no financial liability in case of unauthorised payment.
- Comprehensive record-keeping and auditability: Every agentic payment, along with the decision-making process preceding it, must be recorded to enable thorough auditing. These records should be accessible to any relevant payment user.
- Accountability for agent misconduct: Should an AI agent breach its mandate or facilitate unlawful activities (such as fraud, money laundering, or sanctions circumvention), PSPs should not bear any liability, as PSPs should not be held liable for events outside their control.

Clear liability allocation in case of unauthorised transactions or APP fraud involving AI agents

In order for PSPs to be able to protect their customers from fraud as well as to protect themselves from unwarranted financial liabilities, the impact of agentic payments should be assessed in regards to unauthorised transactions, and APP fraud.

The PSP of the payment service user must not be held accountable for any unauthorised transactions originating from an agent outside of the mandate given by the payment service user. In the case where there is no mandate per se, for instance where the agent anticipates user's requirements and executes transactions seamlessly without real-time prompts, the liability of unauthorised transactions cannot be on the PSP that is not a key participant in the exchanges between the user and the AI agent. The issue may also arise where a user deems a transaction "unauthorised" because the mandate may not have been clear and precise, or there was a misinterpretation or misunderstanding.

Where an AI agent is implicated in APP fraud, the allocation of liability between the agent developer, the deploying firm, and the user requires further assessment as market practices develop and use cases mature, but must exclude PSPs. While the EMA fully supports the adoption of agentic payments to safeguard the UK's position as a dynamic and competitive financial center, it cannot and should not be achieved at the detriment of the PSPs. Therefore, PSPs should be protected from financial liability and accountability regarding the malfunction or exploitation of a third-party AI agent that results in APP fraud.

Question 16: Are there any other innovations across the payments landscape that the Government should take into account when reforming its payment services regulatory framework?

No comment.

Question 17: How can the Government ensure these reforms support an inclusive payments landscape?

The EMA agrees that an inclusive payments landscape is an important objective, and recognises the dual-edged nature of the innovation this consultation aims to address: new technology (flexible payment models, smart data-driven user convenience and authentication tools) has real potential to widen access for currently underserved consumers, but the same pace of change also risks leaving behind those who cannot, or do not wish to, transact digitally.

In fact, the e-money and payments sector has long served underserved communities and customers with vulnerabilities. For example, prepaid and e-money accounts for those unable to access mainstream bank accounts due to credit history, migrant workers or immigrants without access to standard ID documentation; age appropriate accounts giving under-18s tools to develop money management skills; carer cards enabling access by those looking after elderly or other vulnerable customers, and prepaid card programmes used by local authorities and charities to distribute benefits and hardship funds.

Having said that, the UK already has one of the most robust regulatory standards in the world when it comes to inclusivity in payments. This includes the FCA's Consumer Duty, which requires firms to avoid foreseeable harm and design products around customers' actual needs, as well as the FCA's dedicated guidance on the fair treatment of vulnerable customers, in force since 2021. Together, we consider these set high, customer outcomes-focused standards while allowing based on particular circumstances. The EMA's view is that the government's MPR reforms should avoid layering further, payments-specific requirements or duties on top of requirements that already apply and are under the FCA's supervision.

Question 18: What are the key risks which have emerged in the payments and electronic money sector over recent years?

Whilst not exclusive to the payments sector, we address fraud, and Authorised Push Payment (APP) scam fraud risks and suggestions how to tackle them, in response to Q20 below.

Question 19: Would enhanced accountability of senior managers support efforts to manage financial crime risks in the payment services and electronic money sector? Would there be any risks to international competitiveness from this?

The case for smarter supervision rather than new requirements

The EMA fully supports the goals of a regulatory environment that maintains trust and confidence in the payment services sector, supports resilience of the UK's financial system as a whole, and in which decisive action is taken against bad actors. As in any industry, the e-money and payments sector includes good and bad actors with differing standards of compliance, and firms that do not observe existing requirements are unlikely to be brought into line simply by the introduction of further ones. Allowing non-compliant firms to continue operating unchecked also distorts competition, disadvantaging responsible firms who have already made significant investments in the effort to tackle financial crime, bear the cost and effort of compliance and cannot compete on a level footing against firms that do not meet the standards.

That being said, e-money and payment services firms are subject to exactly the same anti-money laundering and financial crime risk management standards as the rest of the financial services sector. The FCA already holds broad FSMA-based supervisory and enforcement powers in relation to firms authorised or registered under the PSRs and EMRs, including the ability to conduct investigations and skilled person reviews, vary or cancel permissions, impose fines, issue public censure, use of voluntary requirements (VREQ) mechanism, and other disciplinary measures against individual managers - a toolkit the government's consultation itself acknowledges at paragraph 3.40. The EMA believes that the FCA should focus on supervision and exercising its existing powers - targeting firms and individuals that show genuine risk indicators and signs of falling short of required standards - rather than the sector as a whole being made subject to a new, generic accountability layer.

Why SM&CR extension not appropriate for the sector

Turning to the idea of enhanced senior manager accountability along the lines of the Senior Managers and Certification Regime (SM&CR), the EMA does not believe this to be an appropriate or proportionate tool for the payment services and electronic money sector, for the following reasons.

Duplication of existing accountability mechanisms and no demonstrated supervisory gap. EMIs and PIs are already subject to regulatory oversight of their directors and senior managers through the existing regime for EMD/PSD Individuals. Firms must already demonstrate that these individuals are fit and proper, and the FCA already has powers to intervene where concerns arise about an individual's conduct or competence.

The consultation does not point to specific supervisory gaps or enforcement outcomes that are traceable to inadequate senior manager accountability. The National Risk Assessment finding cited reflects the sector's overall growth in scale and complexity - not a specific weakness in individual accountability. The consultation also expressly acknowledges that the FCA already has powers to act where firms (or individual managers) fall below the required standards.

Against that background, the relevant question is whether there is a particular accountability gap that contributes to those risks and, if so, what additional mechanism would address it. Absent that evidence, introducing a new accountability regime risks being a disproportionate response to a risk that has not been shown to arise from the cause the proposed remedy addresses.

Poor SM&CR fit for the sector. SM&CR was designed and calibrated for banks, lenders, insurers and investment firms, with materially different products and risk profiles from the EMI/PI population. With close to 1,200 firms authorised or registered under the PSRs and EMRs - a population that includes many small and micro firms - a regime transplanting the existing SM&CR architecture is simply ill-fitted and risks imposing requirements that do not correspond to the business model and the material risks associated with the e-money and payments sector.

A number of elements of the existing SM&CR framework illustrate this difficulty. For example, a significant portion of the regime and in particular certification requirements address risks and roles with little bearing on the EMI or PI business risks, such as remuneration committees, material risk takers, trading, investments or client-dealing functions. Those functions may be appropriate in the businesses for which they were designed but translate poorly to payment and e-money business models, where the risks are fundamentally different and are based on a model of safeguarding funds rather than lending or investing. A transplant based on the existing SM&CR architecture would therefore either produce inappropriate outcomes or require firms to devote considerable time and resources to determining and explaining why particular categories or rules should not apply.

The accountability framework should be based on the risks material to the sector. As noted above, the risks arising from payment and e-money services are materially different from those arising from lending, trading or investment activity. That is not to say payments firms are risk-free, but it does mean the senior management oversight and accountability framework should be built around the material risks for this sector, such as safeguarding, financial crime and operational resilience. It is not suggested, however, that any SM&CR-like requirements should extend beyond key operational oversight roles. For example, customer support staff and technical engineers all contribute to payments operations, but the risks associated with their activities can and are managed through firms' existing systems, controls, and senior management oversight. It would be disproportionate to require every individual contributing to those activities, particularly across group structures, to be mapped into an SMF or Certification like functions.

Disproportionate burdens on both small firms and large international groups. Firms with experience across both the PSD/EMD Individuals regime and SM&CR report significant additional administrative burden in governing and maintaining SM&CR compliance. For smaller firms with limited compliance resources, maintaining detailed Statements of Responsibilities and certification processes, is onerous. For firms with international group structures, where operational functions are commonly shared across group entities and extend across complex group structures, these added administrative burdens are amplified: SMF and Certification Function mapping, maintenance, governance and reporting - whenever reporting lines or responsibilities change. These additional burdens should only be justified if there are clear, additional regulatory benefits to be achieved.

Sequencing with the ongoing SM&CR reforms. It is acknowledged that the HMT and the FCA have already committed to reviewing, and potentially simplifying, aspects of the existing SM&CR regime. As the HMT has itself acknowledged (in [HMT Consultation Response: Reforming the Senior Managers and Certification Regime](#)), after a decade of experience a number of the regime's requirements do not deliver improvements in governance or conduct while imposing unnecessary administrative burden, and the government has committed, jointly with the FCA and PRA, to a 50% reduction in the regime's regulatory burden. Nevertheless, the most significant structural changes needed to deliver practical improvements for firms, such as removing the Certification Regime altogether and materially reducing the population of SMFs requiring pre-approval, are dependent on the Phase 2 reforms. Phase 2 itself includes primary legislation not yet introduced, and their practical shape yet to be determined following the FCA and PRA's Phase 2 consultations. In short, the SM&CR reforms and any improvements they achieve will take time to crystallise, let alone to be embedded in practice. Against this background, the EMA considers it premature to contemplate the extension of the SM&CR regime to an entirely new sector, before the future shape of the SM&CR becomes clear.

On international competitiveness. The EMA believes that extension of the SM&CR regime architecture, including SMF and Certification function-style categorisation, to the payments and e-money sector risks undermining the UK's international competitiveness in this space.

The SM&CR's perceived impact on the UK's financial sector competitiveness is well-documented, including in HMT's own SM&CR [consultation response](#). Respondents to that consultation, including banks, insurers and investment firms, reported the UK being perceived as less competitive due to UK's individual accountability framework, slow cross-border references and checks, which in particular make it difficult to recruit internationally mobile candidates. In addition, the respondents' evidence that obstacles relating to how the SM&CR applies within global group structures will persist even after its reforms are implemented. We share these concerns with respect to the e-money and payment services sector also; if firms already subject to the regime continue to face this unresolved difficulty, the same should be expected, and likely more acutely, for payments and e-money firms encountering the full burden of the regime for the first time.

Finally, applying an SM&CR regime designed for banks and investment firms to EMLs and PIs also risks weakening the UK's competitive standing relative to the EU. The EU's PSD3/PSR continues to regulate payment institutions through a sector-specific framework, ensuring strong governance and oversight standards, but without adopting an equivalent of the UK's SM&CR accountability architecture. Introducing materially more extensive and burdensome individual accountability requirements in the UK could therefore increase the governance and compliance costs associated with locating or expanding payments activities in the UK, costs which their EU counterparts would not face.

Question 20: Are there targeted amendments that could be made to current regulation which would tackle sector risks in a proportionate way?

Whilst not exclusive to the payments sector, fraud, and Authorised Push Payment (APP) scams in particular, remain one of the most prevalent risks facing consumers and PSPs. Fraud cannot be tackled in any meaningful way through action confined to PSPs and banks alone, it requires the fuller involvement of the wider ecosystem in which fraud actually originates, including online platforms where victims are recruited and law enforcement agencies responsible for pursuing perpetrators.

The EMA considers there is scope for two targeted, proportionate initiatives that would meaningfully strengthen the current framework.

Extending accountability to social media and tech platforms. As noted in response to Question 2, the PSR's [fraud originations report](#), published December 2024 using data from the 14 largest UK bank PSPs, identifies the significant role social media and technology platforms play in the recruitment of APP scam victims. Under the current framework, the regulatory and reimbursement burden of APP fraud falls almost entirely on sending and receiving PSPs, despite a substantial proportion of scams originating on platforms outside any PSP's control or visibility. If the Government is to tackle fraud in a proportionate way, social media and technology platforms must be enlisted to play their part in the fight against fraud. Placing the full weight of remediation on PSPs and banks alone, while the platforms where fraud often originates face no equivalent obligation, is neither proportionate nor likely to reduce fraud at its source.

One specific measure that may be helpful to introduce is compelling digital platforms to implement rigorous **merchant identity checks and robust transaction safeguards**, thereby removing a vulnerability that is currently being exploited at scale by bad actors.

Building on the Economic Crime and Corporate Transparency Act 2023 for fraud data sharing. The UK has taken the lead in creating a permissive fraud data sharing environment with the

Economic Crime and Corporate Transparency (ECCT) Act 2023. Previously, firms have been highly reluctant to cooperate and share data due to existing AML and GDPR perceived legal constraints. Therefore, in order to share data firms had to navigate around mostly restrictive legislation that made it an awkward and slow process. The ECCT Act creates new provisions in the Proceeds of Crime Act 2002 (POCA) to enable sharing of information between regulated businesses for the purposes of preventing, detecting and investigating economic crime. It came into effect in November 2023, and is yet to realise its full potential.

The ECCT Act should be used as the basis for enabling broader, coherent information reporting and real-time intelligence sharing across UK sectors - payments, media and telecoms - for the purpose of fighting financial crime. This must be a primary goal for the provision of the industry-wide fraud and claims handling solution. It is not suggested, however, that the government should intervene to mandate data sharing at this stage. The EMA considers that an industry-led approach to data sharing to mitigate the risks of fraud, as opposed to mandating any data sharing requirements or solutions, is the right approach.

Question 21: Do you agree with the proposal to establish a new right of access to support the development of variable recurring payments? If so, what do you think the scope of this new right of access should be – both in terms of the requirement itself and its scope of application? Please explain your answer.

The EMA agrees with the proposal to establish a new statutory right of access to support the development of variable recurring payments (VRP).

We welcome the progress that the UK Payments Initiative's commercial scheme for variable recurring payments (VRP) has made with its launch in June 2026, and the anticipated extension to general e-commerce (in Wave 2).

However, we acknowledge that a critical factor determining whether VRP gains market traction for e-commerce is merchant acceptance. A merchant assessing whether to offer VRP is not just evaluating cost, but also the number of customers who are able to use that payment method. A payment method that fails for a material proportion of their customers imposes a support burden, a conversion loss and a reputational cost that pricing advantage cannot offset. Therefore, VRP schemes must support the widest possible payer access to that payment method, and the statutory right of VRP access supports this outcome.

We also note that Scheme participation is a commercial decision, additional account to account schemes may emerge, and ASPSPs may choose the scheme most suitable to their business. Hence the statutory right of VRP access provides a floor beneath the commercial schemes which ensures

that the capability must be available, while the terms on which it is made available is for the market to determine.

Scope of application of right of access

The consultation identifies two possible limits on scope of application of the VRP right of access: confining ASPSPs providing current accounts, and ASPSPs above a size threshold. We consider that neither of these thresholds support a durable and future proof scope test.

We agree that the ‘current account’ test if applied today would include ASPSPs where the overwhelming majority of payers will initiate VRPs. However, we note that the provision of the types of payment accounts is not static and that limiting the scope to a particular category of payment account, may require amendment in the longer term.

However, as the consultation identifies, authorised electronic money institutions (EMIs) and payment institutions (PIs) that offer payment accounts fall within the definition of ASPSP, including in the context of VRP right of access. Consequently, if the ‘current account only’ scope is discounted we consider that the ‘size’ threshold may produce outcomes which are disproportionate for some EMIs and PIs.

A size threshold drawn by account numbers, or transaction volume, may produce an arbitrary result i.e. two firms of similar size, one whose accounts are the subject of substantial TPP demand and one whose accounts attract none, would be treated identically — and in the second case the firm would be required to build and maintain infrastructure to support VRPs for which there is no demonstrated demand.

Therefore, we propose that ASPSPs should be assessed as within the scope of the new VRP access right based on **demand for access**, or reasonably anticipated TPP demand, rather than by the proposed current account or a size threshold. The FCA should be empowered to make the determination of in-scope ASPSPs based on published criteria on application by an ASPSP; and in-scope ASPSPs should have a defined implementation period before the obligations take effect (if they are not already part of a VRP scheme).

Relationship between VRP access right and paid access

The EMA supports the consultation’s proposal that access for VRPs, other than in respect of sweeping (Q31), should not be required to be free. We discuss our position on the boundary between free services and those services where charging should be permitted under Question 22.

Question 22: What are your views on whether and under what circumstances ASPSPs should be able to charge third party firms for the access which they are currently required to provide for free under the PSRs and CMA Order?

The EMA supports the objective of creating fair and sustainable commercial arrangements for Open Banking going forwards, and appreciate the two aims that the consultation identifies: to protect the business models of PSPs who rely on existing free access to payment accounts, and respond to concerns about the potential for large companies to access free APIs at significant scale.

To achieve both of these aims we consider that payment access falling within the existing Rights of Access in regulations 69 and 70 of the Payment Services Regulations 2017 (PSRs) should remain free of charge. **Charging should only be permitted for functionality beyond that baseline,** including the new right of access for variable recurring payments, subject to the sweeping carve-out proposed by HMT (under Q31).

This approach will allow ASPSPs to genuinely price new capability – variable recurring payments, richer data, guaranteed performance, value-added services – that the ecosystem requires them to invest in to achieve HMT’s objectives for Open Banking, and eventually Open Finance. It also directs the investment incentive at new functionality and infrastructure rather than at the monetisation of infrastructure that has already been established. Hence also achieving HMT’s first aim of protecting existing business models in the market.

We also recognise the impact on ASPSPs when APIs are accessed at significant scale, frequency, and/or both, and the reasonableness of managing that impact. However, we would urge caution in determining that fees for API access should be triggered by volume or size of usage within the current scope of free OB APIs, as this could lead to unintended consequences to the business models amongst the PSPs that HMT also aims to protect.

For instance, a large proportion of PSPs providing TPP services, technically access payment accounts to carry out PIS or AIS through aggregator TPPs i.e. the highest volume API callers are often aggregator TPPs. Any fees for access levied on the aggregator TPPs will likely be passed to the long tail of PSPs using their services. And hence could potentially threaten the business model of those smaller TPPs that the size/volume triggers for fees is aiming to safeguard.

We would also suggest that introducing charging by volume/size triggers for existing OB APIs could affect the provision of AIS more substantially than PIS, because AIS involves more frequent API polling with limited revenue to offset access costs. We urge HMT to model the impact on AIS and PIS services separately if this is a route being considered.

We would suggest that under our proposal for maintaining the boundary of free API access for current baseline functionality, the issue of heavy or unreasonable API use can be addressed by FCA rules, and Future Entity standards.

Uncertainty on FCA discretionary powers

The consultation proposes to enable the FCA to determine whether access currently required to be provided free of charge should transition to a commercial basis. The details of HMT's thinking on the perimeter, or criteria, that will form the basis of the FCA's discretionary powers are not described, nor is a likely timetable for implementation.

We suggest that the open-ended character of the proposals will generate unnecessary uncertainty in the market. A power that may be exercised at an unspecified point, on unspecified grounds, in respect of an unspecified portion of a TPP's current free access is a contingent liability that will be felt by the entire open banking sector and will likely have the effect of slowing investment and progress.

International alignment

In addition, under the political agreement reached on the European Union's revised PSD3/PSR package, data access and payment initiation within the scope of existing PSD2 remain free of charge and cannot be made dependent on a contract, with charging permitted for premium services beyond that scope when under a scheme. Our proposed approach above materially aligns with the European revised framework and as such would place UK TPPs on a level playing field with their European competitors, and supporting UK TPP growth.

Question 23: Are there circumstances in which you think the ban on ASPSPs requiring a contract in regulations 69 and 70 should be lifted?

No, the EMA considers that the **prohibition of requiring a contract** for baseline services under Art 69 and 70 PSRs **must be retained without exception**.

If contracts were not prohibited, it transfers to the ASPSP's discretion whether or not access is available and on what terms. The contract conditions would likely not be confined to price, and non-price items such as data fields available, use of the APIs, permitted use cases, onward data sharing, and terminations rights could all prove catastrophic for some existing TPP business models which runs directly counter to HMT's objective of protecting the existing ecosystem.

Question 24: Are there adjustments that should be made to the Rights of Access as set out in regulations 69 and 70 of the PSRs which would better support Open Banking?

No comments.

Question 25: Are current definitions in the PSRs which are relevant for Open Banking – for example definitions of payment initiation service or account information service – fit for purpose? Please explain.

We have a number of comments on the scope and definitions relating to AIS and PIS, as discussed below. We address some additional PSR definitions that are relevant to Open Banking in the following section, and in our response to Q3.

Scope of AIS definition

Regulation 2(1) defines an ‘account information service’ as an online service to provide consolidated information on one or more payment accounts held by the payment service user with another payment service provider or with more than one payment service provider. This includes whether information is provided in its original form or after processing; and whether it is provided only to the payment service user or to the payment service user and to another person in accordance with the payment service user’s instructions.

We would welcome further clarification on the intention behind AIS and the broad scope of services which could be provided now and in the future.

(i) The current definition reflects the nature of AIS services at the time of drafting of PSD2 and is built around the *output* when account information is accessed i.e consolidated information. Today this only reflects a small part of such services available in the market. We therefore consider it may be helpful to define AIS more broadly as services that involve authorised access to payment account data held by an ASPSP. The current definition restricts innovation in AIS service offerings, by restricting the scope of products that can be offered. It is not suggested, however, that the revised definition should capture a broader set of actors than the party first retrieving account data; it would be disproportionate to regulate all of the parties that may be involved in the data flows.

(ii) The definition of ‘account information services’ also refers to the provision of information on account(s) held with another PSP or more than one PSP. Some PSPs offer accounts that can only be accessed (for example, to view balance and/or transactions) by PSUs via an interface (such as an app) developed and maintained by a third party. It would be helpful to clarify that such third parties are not engaging in account information services when providing account information on behalf of the PSP with whom the account is held.

Scope of PIS definition

Regulation 2(1) currently defines ‘payment initiation service’ as an online service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.

We would welcome clarification on the scope of the PIS definition as follows:

- With regards to the new access right of VRP proposed (Q21), section 4.2 of the consultation refers to the lodging of a ‘payment mandate’, whereas the current definition of payment initiation service refers to the initiation of a ‘payment order’. It would therefore be helpful if HMT could clarify if lodging a mandate, and managing it thereafter, constitutes a payment initiation service (or part of it), or if this is a distinct unregulated activity. We envisage that services may emerge for managing customer’s mandates – lodging, amending parameters, pausing, or revoking – for example as part of using AI agentic tools (see below). In this scenario, a firm could manage a PSU’s mandates without initiating payments themselves (see our discussion regarding the regulatory perimeter for PIS when AI agentic tools are used below).

Future Proofing definitions of AIS and PIS

Finally, with the objective of future proofing the definitions of AIS and PIS, we would urge HMT to consider how the definitions should be interpreted in relation to AI-enabled services. The EMA considers that maintaining the technology-neutral position currently established in the PSRs is essential, but statutory clarification and FCA guidance on how AI-tools fit within the existing regulated activities is equally as critical so that the Open Banking legislative framework does not become outdated as AI technology evolves and its use in the market becomes more prevalent.

We consider some of the Open Banking specific issues relating to AI use below, and also discuss AI issues more generally in our response to Q15.

The current AIS and PIS definitions were drafted with the intention that a regulated firm provides information to, or initiates payments for, a human user. They were not drafted to support the scenario where autonomous software agents act continuously on behalf of the user.

As discussed above, we consider that the core AIS/PIS legislative definitions should focus on the function performed by the third party – authorised access to the payment account, and the parameters for that access. However, we would welcome clarifications on:

- when an AI-enabled service provider is regarded as providing AIS or PIS, rather than supplying technology to a regulated firm or end user;
- the distinction between analytical or advisory AI tools and services that exercise sufficient control over payment account access or payment initiation to constitute a regulated activity;
- how concepts of PSU consent, authentication, and transaction authorisation should operate where payment transactions are initiated by an AI agent within parameters established by the customer;
- the allocation of responsibility and liability between PSU, regulated firms and AI service providers where autonomous decision-making contributes to a payment transaction.

We recognise the risk that the rapid evolution and use of AI technology may require changes to the AIS/PIS definitions in a manner faster than the legislative process allows. We therefore suggest that HMT consider allowing updates to the AIS/PIS definitions through secondary legislation as necessary as the market evolves.

Additional Relevant Definitions

Payment account

Regulation 2(1) PSR defines ‘payment account’ as an account held in the name of one or more payment service users which is used for the execution of payment transactions. The definition of payment account is broad, and given the obligations in relation to regulations 69-70 PSRs on account access by TPPs, this is of key interpretative importance. However, we note that the scope of accounts that are captured is still subject to difference of interpretation, with resulting uncertainty over which accounts are available to PIS and AIS providers. It would be helpful to clarify the scope of the definition of a payment account, and for this to be set out in a pragmatic manner.

We discuss the definition of ‘payment account’ further in our response to Q3.

“Accessible online” or “online access” in the context of the PSRs

Regulation 69 and 70 provides the right to make use of a payment initiation service provider or an account information service provider. The right does not apply where the payment account is not ‘accessible online’.

Art 31 of UK RTS on SCA requires that ASPSPs offering payment accounts that are ‘accessible online’ shall provide a dedicated interface for third parties to access those accounts.

The phrase ‘accessible online’ is not defined in the PSR definitions and has led to market uncertainty as to when account servicing payment service providers are required to have in place a dedicated access interface to a payment account that can be used by authorised third party providers (AISPs, PISPs, CBPIIs). Further clarification could leverage existing text that appeared in Recital 95 of PSD2, and would read as follows: *“services offered via the internet or via other at-distance channels, that enable access to the payment functionality offered by the PSP through any channel and which do not depend on where the device used to access the payment account or initiate the payment transaction are physically located.”*

Regulation 2(1) defines ‘**Sensitive payment data**’ as data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.

We note that despite this clarification for AIS and PIS, the absence of further definition of “sensitive payment data” has led to diverging interpretations and given rise to some ASPSPs taking a risk-averse approach to the data made available to TPPs, with some ASPSPs opting not to provide the name of the account owner and the account. Further specification of ‘sensitive payment data’ would remove ambiguity, and provide a clear perimeter for the data that must be provided to TPPs.

Question 26: Are there any requirements related to Open Banking within the PSRs that you consider should remain in legislation, as opposed to responsibility for the requirement being given to the FCA?

The EMA supports the delegation of rule-making powers to the FCA with regards to Open Banking provisions, to encourage a flexible and agile evolution of Open Banking services. Provision of Open Banking requirements across primary legislation, the SCA-RTS and the CMA Order has proved cumbersome for a market that continues to develop and is required to support the expansion of OB services that the Government envisages.

As a general principle, we consider that requirements conferring a right or protection on a market participant or PSU should stay within the PSRs, while FCA Rules and Future Entity standards tackle technical and operational obligations.

In summary, we suggest the following remains in legislation:

- The rights of access in regulations 69 and 70, including the new right of access supporting variable recurring payments.
- The prohibition on requiring a contract as a precondition of access (see our response to Question 23).
- The principle governing what may and may not be charged for, as distinct from the level of any charge or the methodology by which it is set (see our response to Question 22).
- The allocation of liability between ASPSPs and TPPs, including in respect of unauthorised and incorrectly executed transactions initiated by a PISP.

As discussed in our response to Question 27 below, we believe that several elements adopted in the EU PSD3/PSR framework could provide useful additions to the Open Banking obligations in the UK PSRs.

We note that the consultation frames the choice between obligations being made in legislation and FCA Rules. In practice, following these reforms, an Open Banking obligation may arise from any of four sources: the PSRs; FCA rules made under powers conferred by the Data (Use and Access) Act 2025; standards set by the Future Entity (if mandated use); and the rulebooks of commercial schemes. The burden of these four layers of obligations needs to be considered, particularly for

smaller ASPSPs, and we would welcome confirmation that the cumulative effect across the PSRs, rules made under Data (Use and Access) Act powers, Future Entity standards and commercial scheme rulebooks will be assessed as a whole.

Question 27: Are there any other adjustments needed to current regulation which would better support Open Banking?

The regulatory framework for AISP and PISP has enabled new entrants to offer innovative services, in turn, encouraging growth and competition in the market. There have been, however, associated difficulties which undermine these outcomes, and we suggest some additional requirements at the legislative level could help to improve the functioning of the UK Open Banking market.

Level-playing field for gaining AIS/PIS permissions

The restrictions on AIS and PIS permissions set out in the current EMR and PSR distinguishes the authorisation process for authorised EMLs and PIs seeking to offer AIS and PIS services, from that for credit institutions. In order to be able to offer these services, EMLs and PIs must obtain approval of their application for variation in permissions, while credit institutions are only required to notify the FCA. The process, whether it amounts to notification or variation of permission, should be identical for all institutions, in order to avoid giving an advantage in speed to market and cost to credit institutions.

Exemption from providing an interface

A blanket requirement to provide access to all payment accounts held by all account providers has resulted in unintended consequences. ASPSPs have faced significant costs in developing compliant access interfaces. This has had particular impact on smaller ASPSPs who may not have experienced demand for account access, particularly from the AIS ecosystem. Some of our members have implemented, and now maintain, PSR compliant interfaces and report no demand at all for access from TPPs.

We, therefore, consider that there is an opportunity to introduce a “demand” threshold below which ASPSPs could operate payment accounts without having to provide TPP access. This could also be coupled with an exemption process for ASPSPs who can duly evidence that the payment accounts they offer do not meet the demand thresholds from TPPs for access. A similar proportionate approach has been adopted in the EU PSD3 legislative package, and we consider that the derogation from providing an interface should be introduced in the reformed PSRs rather than secondary FCA Rules so as to simplify the scope of ASPSPs mandated to participate in the Future Entity standards (see our response to Q28).

Obstacles to providing TPP services

Article 32(3) of the RTS on SCA and CSC currently prohibits ASPSPs from creating "obstacles" that hinder TPPs from offering AIS and PIS. Since the introduction of the RTS, the market has struggled to define what is, and what is not, an obstacle, and ensure consistent open banking journeys are implemented for users. For this reason, we conclude that the prohibition on obstacles to account access as a principle should be elevated to first level legislation, with any specific, market blocking obstacles being enumerated and managed in FCA Rules.

Question 28: Do you agree with the proposed approach to provide the FCA with powers to place interface-related requirements on ASPSPs, PISPs and AISP?

The EMA supports the proposed approach to providing the FCA with powers to place interface-related requirements on ASPSPs, PISPs, and AISPs, including the implication that the FCA could mandate the use of Future Entity standards for baseline services under regulations 69 and 70 of the PSRs. The use of a single standard amongst the largest ASPSPs (CMA9 banks) has played a significant part in driving adoption of OB services in the UK, and allowed the UK to outpace other markets. The move to extend adoption of Future Entity standards provides an opportunity to further drive this advantage, and reduce fragmentation between interface deployments and hence customer journeys.

ASPSPs required to use Future Entity standards

However, we note that extending the scope of participation in the Future Entity (FE) standards will not be without impact on the existing market. In particular, ASPSPs who are not currently using Open Banking Ltd's interface standards will face migration and on-going costs. We would therefore welcome further analysis of the impact of mandating Future Entity standards on the whole market, and in particular, with regards to the funding and governance of the Future Entity.

As discussed, in our response to Q27, the availability of a legislative exemption from providing an interface could provide a proportionate solution for those ASPSPs facing no demand for access to their accounts. FCA Rules could also establish the "demand" thresholds as one of the metrics used to determine which ASPSPs must use FE standards.

Funding determination power

The power to determine which firms must fund the Future Entity is the power which has the greatest potential to affect smaller participants on both sides of the market, and therefore we propose that it cannot be delegated without constraint.

We suggest that the instrument conferring the funding determination power requires that the FCA apply a proportionate funding formula, including:

- a floor below which firms do not contribute, or contribute at a nominal level;
- tapering by reference to size, transaction volume or access volume;
- a mechanism to avoid double contribution by firms subject to obligations on both sides of the market; and
- consultation before any determination, and before any material change to the formula.

Question 29: What are your views on whether the FCA should be provided with a power to mandate ASPSP participation in commercial Open Banking schemes?

The EMA suggests that the FCA is provided with reserve powers to mandate participation in a commercial scheme which are exercisable only when statutory conditions are met, such as lack of payment account coverage for a scheme which is central to government payments policy. In other words, the powers provide a quantifiable backstop which can be used to break a deadlock if market participation in a commercial scheme stalls.

In the first instance, we believe that the reserve powers could extend to just the commercial VRP scheme, with published quantified thresholds being set – such as coverage of in-scope accounts by a stated date, with the power falling away if the thresholds are met. We discuss an option regarding further FCA powers to encourage VRP scheme participation without the need for the FCA to exercise the suggested reserve powers and support scheme participation in our response to Q34.

This approach is to mitigate against significant delay or impact on the market if legislation changes are required to grant the FCA powers retrospectively when a scheme's progress is waning. It could also prevent the scope of participating ASPSPs in a commercial scheme being restricted by the incumbent members when the scheme is necessary to meet the government's payments policy objectives.

Question 30: Would it be beneficial to maintain a requirement on ASPSPs to publish product and reference information via Open Banking APIs, as is required today under the CMA Order?

No comments.

Question 31: Would it be beneficial to maintain a requirement on ASPSPs to enable sweeping variable recurring payments, as is required today under the CMA Order?

The EMA supports maintaining the requirement on ASPSPs to enable sweeping VRP, and we suggest that the free-of-charge treatment of sweeping is preserved as it supports use cases with a direct consumer benefit — the automated movement of funds between a customer's own accounts to

avoid unarranged overdraft charges, to move balances to better-remunerated accounts, or to manage repayments.

We also observe that sweeping has served as the proving ground for VRPs which are now being commercialised. Allowing the requirement to lapse at the point the commercial layer is emerging into the market could fragment services offered to end-users.

Scope of application

We consider that the ASPSPs currently mandated to provide sweeping under the CMA9 Order should remain so under the new arrangements. However, we recognise that maintaining this scope may leave customers of other institutions outside the nine banks without a capability they may find valuable if their ASPSP does not voluntarily offer the service.

If HMT is considering widening the scope of ASPSPs mandated to provide sweeping beyond the CMA9 banks, we suggest that the in-scope ASPSPs be determined by the same 'demand-test' proposed in our response to Q21. This will ensure that ASPSPs who actively see TPP demand for access to their payment accounts for sweeping are required to make the capability available, and protect those who see no demand from TPPs at all.

Finally, we suggest that the requirement to provide free of charge sweeping services is carried forward in statutory instrument, rather than being delegated to FCA Rules. This will protect the longer term provision of these services which are low-margin, but generate value for the end customer.

Question 32: Do you agree with the proposed approach to providing the FCA with powers to regulate the Future Entity as an interface body?

No comments.

Question 33: Do you consider there would be any competition law barriers to the operation of commercial Open Banking schemes under the proposed approach and, if so, how might these be addressed?

We urge HMT to prioritise resolving the competition law uncertainty surrounding pricing within commercial Open Banking schemes, and to do so through whichever legal or regulatory route can deliver durable certainty quickly. Until a lasting solution is in place, PSPs face a choice between investing in schemes whose commercial model may later be challenged, or holding back, at the cost of the coverage and adoption of account to account payments that the Government anticipates in the National Payments Vision. We would welcome a clear commitment from HM Treasury on how

and when this will be resolved, and an assurance that current interim arrangements for the commercial VRP scheme will continue uninterrupted if the long-term framework is not in place before the current arrangements expire.

Question 34: Do you agree that the FCA should have powers to intervene directly in the pricing of Open Banking access arrangements where necessary? Should those powers differ depending on whether the pricing arrangement is established through a commercial scheme or outside a commercial scheme? Please explain your answer.

Commercial scheme pricing

Assuming that the approach described in our response under Q22 and Q23 is established, and charging for access for baseline services under Regulations 69 and 70 PSRs is prohibited, the EMA agrees that the FCA should be given the powers to require each commercial Open Banking scheme which emerges to provide services beyond that baseline, to establish a centralised pricing model, set guardrails for the scheme pricing, and be given the powers to intervene more directly if there are concerns about a scheme's pricing model in the market.

VRP Commercial Scheme

In the context of the emerging VRP scheme, HMT may also want to consider the option that the FCA could be empowered to provide that an ASPSP may charge for access supporting VRP only where that charge is made through a designated commercial scheme.

The effect would be that an ASPSP remains free to decide whether to participate in a VRP scheme, but may not charge for VRP access outside one. Access would continue to be available as a matter of the statutory right in either case.

We recognise that this option is not without risk of impacting smaller ASPSPs disproportionately, and we do not regard this as an alternative to the backstop power we propose in our response to Q29, and would not want it to be adopted on that basis. However, this option does address ASPSP incentive to price outside of a scheme and the fragmentation in the market that this will cause, and potentially strengthens the competition law solution that HMT suggests at Q33 (where the exclusion in paragraph 5 of Schedule 3 to the Competition Act 1998 operates where an arrangement is required by a legal requirement).

To mitigate against the risk identified above to smaller ASPSPs, we consider that if the FCA were given the power to restrict charging for VRP access only through a designated commercial scheme, a series of supporting conditions would also need to be adopted, including:

- **De-minimis exemption** – an ASPSP below a specified threshold of access volume or VRP volume should be able to charge for access without participating in a scheme.
- **Non-discriminatory participation criteria and proportionate scheme fees** - that a scheme's participation fees be proportionate to the size and volume of the participant; and that an applicant refused admission must have recourse to a route independent of the scheme itself.

Out of scheme pricing

Whilst not our preferred course, as discussed in our response to Q22, if HMT decides to permit ASPSPs to charge for account access for what we are referring to as 'baseline services' when certain thresholds are met, we consider that the FCA should also be given powers to monitor and intervene in such pricing if necessary. Arguably, in these circumstances, the FCA's powers should be different, as pricing will likely be outside of a scheme, and potentially impact the entire existing Open Banking ecosystem which has arisen out of free account access for these services.

Commercial schemes operating a centralised pricing model have several features that constrain pricing before FCA intervention would ever be required i.e. pricing is set using a transparent methodology and applies to all participants on the same terms. The arrangement will be visible to the FCA, as they oversee the scheme operator as an interface body under the DUAA. In addition, governance and non-discriminatory participation criteria will be subject to FCA rules, and participants will have a dispute resolution process.

Outside of a scheme, an arrangement has none of these features and the asymmetry in negotiating positions between ASPSPs and TPPs becomes acute. Therefore, in the case where baseline services could be charged for, the FCA should have powers to ensure pricing is transparent, and negotiated on a fair, reasonable, and non-discriminatory basis.

Question 35: Do you agree with the proposed approach to providing the FCA with powers to regulate commercial Open Banking schemes?

No comments.

Question 36: Are there additional powers in relation to participating firms (ASPSPs, PISPs and AISPs), the Future Entity or commercial schemes that the FCA might need to effectively manage Open Banking into the future?

No comments.

Question 37: Do you agree with the proposed approach of mirroring as closely as possible the FCA's monitoring and enforcement powers as set out in FSMA?

No comments.

Question 38: Do you have views on the FCA being given a power to issue compliance notices to enforce compliance with requirements made under DUAA?

No comments.

Question 39: Do you envisage scenarios where it would be helpful for the FCA to share certain confidential information with the Future Entity, in connection with the FCA's role as regulator for Open Banking?

No comments.

Question 40: Do you agree with mirroring the FCA's FSMA objectives and matters to which it must have regard for the purpose of the FCA exercising its new powers and functions in relation to Open Banking?

No comments.

Question 41: What are your views on providing the FCA with an additional objective which reflects the broader data-focused aims of DUAA to support its approach to regulating Open Banking?

No comments.

Question 42: Are there any other areas of feedback on issues raised in this consultation?

No comments.

Members of the EMA as at October 2026:

3S Money	Moorwand Ltd
Airbnb Inc	MuchBetter
Aircash	myPOS Payments Ltd
Airwallex (UK) Limited	Navro Group Limited
Amazon	Newrails, UAB
American Express	Nium Solutions Limited
Aplauz NL B.V.	Nuvei Financial Services Ltd
Banked	OFX
BCB Digital Ltd	OKX
Bitstamp	OpenPayd
Blackhawk Network EMEA Limited	Owl Payments Europe Limited
Boku Inc	Papaya Global / Azimo
Booking Holdings Financial Services International Limited	Park Card Services Limited
BVNK	pay.cetera B.V.
Bytedance Payments	Payhawk Financial Services Limited
Cardaq Ltd	Paymentsense Limited
CashFlows	Payoneer Europe Limited
Circle	PayPal
Coinbase	Paysafe Group
Currenxie Technologies Limited	Paysend EU DAC
Decta Limited	Peratera UK Ltd
Deel	Plaid B.V.
eBay Sarl	Pleo Financial Services A/S
ECOMMPAY Limited	PPS
emerchantpay Group Ltd	Push Labs Limited
EML Payments	Remitly
EPG Financial Services Limited	Revolut
eToro Money	Ripple
Etsy Ireland UC	Satispay Europe S.A.
Euronet Worldwide Inc	Securiclick Limited
Finance Incorporated Limited	Segpay
Financial House Limited	Soldo Financial Services Ireland DAC
FinXP	Square
First Rate Exchange Services	Stripe
Fiserv	SumUp Limited
Flywire	Syspay Ltd
Globepay Limited	TransactPay
GoCardless Ltd	TransferGo Ltd
Google Payment Ltd	TransferMate Global Payments
IDT Financial Services Limited	TrueLayer Limited
iFAST Global Bank Limited	Uber BV
Imagor SA	Unzer Luxembourg SA
Kraken	Vitesse PSP Ltd
Loodapay LU S.A.	VIVA WALLET.COM LTD
Modulr Finance B.V.	Weavr Limited
MONAVATE	WEX Europe UK Limited
MONETLEY LTD	Wise
Moneyhub Financial Technology Ltd	WorldFirst