Electronic Money Association
Crescent House
5 The Crescent
Surbiton, Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
www.e-ma.org

Andrew Clemo
Senior Policy Advisor - Payments
Payments and Fintech Team
HM Treasury
1 Horse Guards Road SW1A 2HQ

21 April 2023

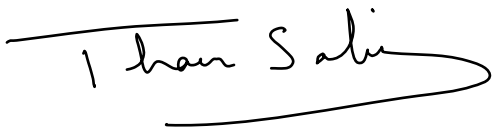
Dear Andrew

Re: EMA response to HMT Payment Services Regulations Review and Call for Evidence

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.

Thank you for taking our comments into consideration.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

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

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

B. Ensuring appropriate trust and protection for consumers

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

D. Fostering competition, in the interests of consumers

In answering the above, the government would welcome concrete reflections from stakeholders for future policy, rather than the principles which should underpin regulation/regulatory change.

Balanced and agile regulation

1. The evolution of the UK payments regulatory framework, as currently primarily set out under the Electronic Money Regulations 2011 ("**EMR**") and the Payment Services Regulations 2017 ("**PSR**"), will require careful balancing and prioritisation of the objectives the government has set for payments regulation outlined in this Review. We envision tensions occurring between different objectives of ensuring market resilience and integrity, achieving regulation which promotes the international competitiveness of the UK economy through growth and innovation of the UK payments sector, and protection of consumers. It is important that the future policy takes account and balances all of these objectives, taking into account the impacts not only in the immediate but also the long term. We consider that agility - the key principle for payments regulation outlined in this Review - will be necessary in the government's ongoing analysis and review of the risks and trade-offs between the government's stated objectives for payments regulation.
2. We reflect on the vast array of recent policy and regulatory changes and initiatives affecting the payments sector, and the gradual extension of the regulatory frameworks traditionally designed for other financial services industry participants, such as credit institutions or investment firms. However, electronic money institutions ("**EMIs**") and payment institutions ("**PIs**") do not, generally, engage in deposit taking activities or investment services and the risks associated with the payment and e-money services are different. We submit that, to achieve proportionate and agile regulation, the rules applicable to EMIs and PIs should continue to be tailored to risks associated specifically with payment services and e-money, taking into account their differences from other financial services and their providers, such as banks.

[1] The Payment Services Regulations 2017, The Electronic Money Regulations 2011, Cross Border Payments Regulation, as amended in UK law, legislation.gov.uk

3. The perception within payments industry is that the regulatory environment is becoming increasingly complex and the regulatory burden on firms is steadily increasing, disproportionate to the actual risk to consumers and the wider financial system that many payment service providers ("**PSPs**") and their products pose. This is likely to disproportionately affect the new or smaller payment sector actors, creating barriers to entry, and adversely affect innovation (e.g. by limiting the ability to introduce or invest in new products and services) and growth of the UK sector in the long term. We therefore welcome the government's commitment in this Review that in considering the replacement of the retained EU law in payments "policy changes will only occur where there are concrete benefits or risks, and not for its own sake". We would urge the government to resist introducing additional regulation, unless the need for it is justified by solid evidence and assessment of its impact and benefits. Avoiding overregulation requires vigilance, as its impact is broad and can be significant.

4. As highlighted in the Review, the future payment services framework will involve a balanced delegation of the firm-facing rules to the Financial Conduct Authority ("**FCA**"), to enable a more agile framework. The principle is welcome. However, to ensure an agile regulatory approach in practice, we consider it is equally paramount to ensure that any regulator (including the FCA) directly facing regulated markets and firms is appropriately resourced, both in terms of number of staff, as well as suitable expertise required. In addition, effective accountability and scrutiny processes are necessary in order to help identify and address regulatory processes and policies that do not meet the stated objectives. To the extent that the FCA is tasked with developing future payments regulation, we consider it important that the FCA's objectives are aligned with the government's objectives as set out in this Review, and that they are subject to oversight and scrutiny in developing that regulation.

Impact of divergence from the EU legislation and international standards

5. The UK payment sector does not operate in isolation. It will be impacted by ongoing worldwide developments as well as changes in the EU regulatory environment, such as the European Commission's review of the Second Payment Services Directive ("**PSD2**") (expected to result in PSD3), new Markets in Crypto-Assets Regulation ("**MiCA**") and the Digital Operational Resilience Act ("**DORA**"). Ensuring international competitiveness for the UK economy through growth and innovation of the UK sector, so that the UK remains the "leading force in global fintech", will require ongoing consideration of global standards, including EU legislation. In particular, this includes an ongoing review of the impact the UK divergence or alignment has on UK firms operating internationally. In that regard, some of our members have expressed a preference for alignment with the EU legislation, such as future reiteration of PSD2, where it brings a demonstrable benefit. For example, the benefits of alignment may include the reduced regulatory and operational complexity, and cost, when compared to operating across diverging regimes. We ask the UK government to continue to analyse the impact of such divergence (or alignment) throughout the development of its future policies affecting the UK payments sector.

Participation in the Single Euro Payments Area ("SEPA")

6. The UK's continued participation in SEPA as a third country remains very important for the UK payments sector. Many payment service providers and their customers rely on SEPA for fast and cost-effective cross-border payments. Consequently, we consider that ensuring the ongoing participation in SEPA should be one of the UK government's priorities. In that respect, noting the UK's desire to remain a member of SEPA and the fact that PSD2 is one the laws that underpins the legal framework for SEPA, we would welcome further clarity on how much variation can the UK government introduce regarding payment services that is materially different from EU law, e.g. the current PSD2 and the future PSD3.

Access to bank accounts and de-risking

7. Non-bank PSPs continue to face difficulties opening and holding on to accounts with credit institutions (banks), and most are subject to increasing de-risking practices. This issue is particularly acute in relation to safeguarding accounts which are a necessity for doing business for most EMIs and PIs. The limited number of banks willing to offer safeguarding accounts poses a barrier to entry for non-bank PSPs; where safeguarding account services are available, they are typically very expensive. The withdrawal of a bank's account services (de-risking) causes a significant disruption to non-bank PSPs. While regulation 105 PSR regulates access to banks' payment account services by PSPs, we consider the regulatory framework for those services has not been operating efficiently. The current situation creates barriers to entry for PIs and EMIs that may provide competing services, distorting the competitive landscape in favour of legacy banks.

8. We consider the government should work to improve the requirements for non-bank PSP access to bank account services, to further the government's objectives for growth and innovation in the payments sector. [2]

9. To improve the situation, we suggest that regulation 105 PSR could be amended as follows:

   - The access to banking services should be a right for PSPs, and/or the appropriate regulator (FCA and the Payment Systems Regulator), as co-competent regulators currently) should be mandated to intervene where no banking services have been forthcoming;
   - The assessment of a bank account application from a PSP should have distinct criteria that favour granting an account, and this should not be a solely commercial matter.

[2] EMA's position on regulation 105 PSR is independent of and without prejudice to its position on access to payment systems, as previously expressed in its response to HMT's consultation on Payments Regulation and the Systemic Perimeter.

The latter, together with compliance related arguments have resulted in an absence of banking services for PIs and EMIs, and particularly those being established;

- Banks should be subject to a higher duty when justifying the refusal to offer account services to PSPs, as distinct from other businesses. The criteria for meeting this duty should be supported by further regulatory guidance;
- FCA and/or PSR should be obliged to publish data on the number of PSPs that are de-risked or refused an account at the application stage.

10. 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.

11. Finally, the difficulty in obtaining and holding on to bank accounts affects not only EMIs and PIs but also cryptoasset firms. As cryptoasset service providers are gradually brought within the UK regulatory perimeter, their need for specifically designated bank accounts (e.g. for client money) or banking services is likely to increase, where the market offering for such services may not be forthcoming. Therefore, we consider that a similar regime may be necessary for access to bank account services by regulated cryptoasset service providers.

Safeguarding

12. We note the government's intention to transfer the responsibility for developing and delivering the safeguarding regime to the FCA (within its firm-facing rules), and that the FCA is invited to consult on changes to the safeguarding regime later this year. The EMA urges the government, as well as the FCA, to consider and consult on any changes to the safeguarding requirements, including on the appropriate balance of delegation of powers in that regard to the FCA, carefully, especially considering the FCA's ability to change its requirements relatively quickly. Safeguarding forms a core part of the regulated e-money and payment services regime, and the financial, business and operational impact of making changes to the regime is likely to be significant.

13. However, the EMA does invite the government, as well as the FCA, to make improvements in the safeguarding rules in the areas set out below. These issues have long posed significant challenges to EMIs and PIs, hindering their ability to manage or diversify risks, placing barriers to entry and putting these firms at a significant competitive disadvantage, which of course ultimately undermines innovation, growth and competition. We consider these issues should be addressed as a matter of priority.

(1) Investment in secure, low risk assets

14. EMIs and PIs are permitted to safeguard funds by investing relevant funds in "secure, liquid assets as the FCA may approve" (regulation 21(6)(b) EMR and regulation 23(6)(b) PSR). Firms need greater clarity regarding the type of secure, liquid and low risk asset in which safeguarded funds can be invested. There is a need for diversification and proportionate flexibility to enable a limited revenue to be generated in order to contribute to the cost

of safeguarding. The assets that firms 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.

(2) Insurance or comparable guarantee option

15. EMIs and PIs are also permitted to safeguard the relevant funds by ensuring they are covered by an insurance policy or a comparable guarantee (regulation 22 EMR and regulation 23(12) PSR). However, safeguarding by insurance is not relied upon much and there appears to be very little uptake so we consider a review of the underwriting conditions is needed in order to resolve the market challenges. The FCA's current expectation that the insurance cover all risks, including risks that would otherwise not be covered by other safeguarding methods, has further increased the cost of such insurance, where there is appetite within the insurance industry to develop such a product.

(3) Safeguarding accounts at the Bank of England ("BoE")

16. As noted above, PIs and EMIs continue to experience de-risking practices, and this is particularly acute in relation to safeguarding accounts. EMIs and PIs should be permitted to safeguard customer funds at central banks, removing investment risk altogether, and assisting in the resolution of part of the de-risking challenges that are faced by the industry. Allowing EMIs to earn the BoE's base interest rate on funds held at the Bank - a benefit currently enjoyed only by credit institutions - would also allow EMIs to better compete with incumbent banks, creating a more level-playing field across the industry on BoE access.

17. The regulations permit EMIs and PIs to safeguard the relevant funds in an account held with the BoE (regulation 21(2)(a) EMR and regulation 23(6)(a) PSR). However, in practice there are significant limitations to the accounts EMIs/PIs can hold with the BoE, which undermines their utility for the purposes of safeguarding.

18. In 2019 the BoE consulted on opening up access to its balance sheet. In its response (Box K: Access to Balance Sheet Review), it recognised the competition and risk reduction benefits of allowing non-bank PSPs to safeguard at the BoE. It also laid out some conditions to be satisfied in order for the BoE to be comfortable with holding client money directly, in light of the risks associated with a potential disorderly failure of a non-bank payments firm:

    (1) Customer funds to not only be 1-for-1 backed at all times, but for appropriate buffers and/or capital requirements to be in place to absorb unexpected losses.

    (2) Protections for customers to be in place to guarantee that all funds are returned promptly to customers in the event of a firm's failure.

    (3) Formal wind-down plans should be maintained to reduce the risk of disorderly failure.

19. The EMA considers these conditions have now been largely addressed, including via (1) additional FCA's guidance and requirements on prudential risk management and assessment of capital adequacy as set out in its Approach Document and Finalised Guidance FG 20/1; (2) the introduction of the Payment and Electronic Money Institution Insolvency Regulations 2021, improving the customer experience and return of customer funds in the event of insolvency; and (3) the FCA's guidance and requirements for wind-down planning, as set out in its Approach Document.

20. Accordingly, the EMA believes that it would be appropriate for BoE to revisit its position and accounts available to non-bank payments firms in order to (i) upgrade the settlement account functionality to allow access to overnight reserves; and/or (ii) create new types of accounts for safeguarding customer funds with BoE. The EMA requests that the HMT and the FCA work with the BoE in addressing these proposals.

(4) Clarifying the status of safeguarded funds

21. Legislation should also clarify that the safeguarded funds of PIs are customer funds held by PIs on behalf of their customers, while the safeguarded funds of EMIs are owned by the EMIs themselves. The absence of this distinction has led to legal uncertainty about the ownership of funds in the context of insolvency.

22. In relation to the funds held by EMIs, there is no legal basis to suggest that e-money holders have any beneficial / proprietary interest in the funds held by an EMI. In fact:

    - e-money holders purchase e-money, a dematerialised financial instrument that represents a claim against the issuer. The e-money holder has a full title to the instrument, and cannot also have a claim on the price paid for it - the funds now held by the EMI;
    - the claim against the e-money issuer is personal and not proprietary. This is apparent from the definition of "electronic money" in regulation 2(1) EMR as *"...value … as represented by a claim on the electronic money issuer…"*. The e-money holder's claim is a claim against the issuer for redemption, not to the safeguarded funds. This is also true when a credit institution issues e-money; there are no safeguarding obligations in legislation, and users have no rights over any asset held by the bank; they do however have the same right of redemption against the bank.

Statutory trusts

23. Following the Court of Appeal's judgment in *Ipagoo*,[3] it is now settled that the EMR do not create a statutory trust in favour of e-money holders and, further, that the imposition

[3] *Baker & Anor v Financial Conduct Authority (Re Ipagoo LLP)* [2022] EWCA Civ 302 (9 March 2022)

of a statutory trust is not necessary to achieve the protection afforded by regulation 24 EMR (for the e-money holders' claims to be paid in priority to all other creditors), including in the circumstances where the funds have not been safeguarded by the EMI. In light of *Ipagoo*, we consider the courts might now similarly conclude that the PSR does not create a statutory trust, despite conflicting earlier judgments from lower courts.[4]

24. We note the government's comments that the Ipagoo judgment has *"highlighted ambiguity within the safeguarding regime that is best addressed ex ante through clearer regulation"* and that the findings made therein "*raised additional issues regarding the insolvency process, potentially adding further to the cost, and time burden, and risk of consumer harm, with insolvency practitioners likely to continue to seek Court directions on these areas of ambiguity.*" We would welcome further clarity on what those additional issues are. The EMA supports the principle of clearer regulation, to provide more clarity to firms and insolvency practitioners alike in a more agile way and to facilitate a more efficient insolvency process. However, it is paramount that any changes proposed are subject to a considered consultation process that provides sufficient information on the issues the proposed changes are intended to resolve. Such detail has been found lacking by the industry in relation to safeguarding related consultations in the past,[5] which undermined the industry's ability to respond in a considered manner, including on whether alternative, and potentially more proportionate, solutions may be available to achieve the desired result.

25. Finally, we note the government's comments make comparisons to the FCA's client assets regime for firms authorised under Financial Services and Markets Act 2000 (FSMA), which is based on a statutory trust over a firm's client money implemented via the FCA's rules, namely the Client Assets Sourcebook (CASS). The EMA calls for a cautious approach to any safeguarding regime changes, including should the FCA consider imposing a similar statutory trust regime as regards the funds held by EMIs and PIs. Any changes in this regard should be substantiated by evidence that the current arrangements are not working and that the reduced flexibility of a client money arrangement (or any other arrangements within the FCA's contemplation) has substantial benefits over alternative options.

26. We consider the imposition of a statutory trust could lead to severe adverse implications for the industry. For example, the 'trust' model necessitates a significant number of restrictions being placed on the safeguarding account, increasing the complexity in the administration and operation of safeguarding accounts, beyond what is necessary to achieve the protections afforded by the current legislation. This complexity would add to the cost of business for EMIs, and erode their competitiveness, compared to credit institutions that issue e-money. It is also perceived that the imposition of a trust over

[4] *Re Super Capital Ltd* [2020] EWHC 1685 (Ch) and *Re Allied Wallet* [2022] EWHC 402

[5] For example, with the FCA's Consultation on Coronavirus and safeguarding customers' funds guidance and the HMT's Consultation on Insolvency changes for payment and electronic money institutions.

funds held in safeguarding accounts may affect the relationship with banks with whom such accounts are held, depending on the bank's risk appetite and perceived obligations with respect to holding funds beneficially owned by third parties (rather than the firm). This could further exacerbate the de-risking problem and the difficulties faced by EMIs and PIs in opening and maintaining safeguarding accounts.

27. In addition, we consider it is important to ensure that any changes to the safeguarding rules do not prejudice the continued availability of any other safeguarding means (such as insurance or comparable guarantee) to EMIs and PIs.

28. In conclusion, we urge the government, as well as the FCA, to carefully analyse the impact of making any material changes to the safeguarding regime, and to engage with the industry in determining an approach that achieves an appropriate balance between the government's objectives for payments regulation stated in this Review.

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

29. The EMA welcomes rationalisation of the e-money and payment services regimes to the extent that it combines the two authorisation and supervisory frameworks, but strongly cautions against any changes to the definition of e-money or the concept of electronic money at law. The e-money industry is long established and the commercial agreements that are in place, make use of the attributes and legal characteristics of e-money to create payment solutions, products and services. Any change in that respect could have broad implications for existing businesses as well as future innovation.

30. We do wish to see a more consistent approach to authorisation and regulatory permissions that allows regulated institutions to offer both payment services and to issue electronic money without having to seek an entirely different license. In other words, a firm offering payment services could apply to vary its permissions to add electronic money issuance to its portfolio of payment products, while adopting the additional regulatory obligations that will ensue, but doing so within the scope of their existing license.

31. Provided that the existing regulatory treatment of e-money is carried through, combining the EMR and PSR could be appropriate, if it brings a demonstrable benefit. For example, if it makes it easier for e-money firms to apply the rules relating to related and unrelated (to e-money) payment services, and removes the requirement to safeguard funds relating to such services separately. This would alleviate the operational difficulties and costs of separate safeguarding arrangements and accounts, where obtaining and maintaining safeguarding accounts still remains an issue for the industry - see our response to Q1.

The regulatory concept of electronic money

32. The e-money industry is a mature industry that has been applying the e-money regime for some 20 years. The concept of e-money is embedded in the UK (as well as the EU)

payments sector, in its commercial arrangements, in its contractual structures, and plays a key role in numerous product propositions and business solutions. The financial and business impact of making any changes to the concept of e-money would be entirely disproportionate to any benefit that can be conceived.

33. The issuance of e-money does not involve the provision of a payment service - it is the creation of electronic value that represents a claim against the issuer. The use of e-money to make payments is a separate activity, and is adequately addressed by existing payment permissions that e-money issuers have.

34. E-money is a separate financial instrument in the same way as deposits are, or the issuing of credit, both of which can also be used to make payments that are subject to the PSR. Similarly to deposits or credit, e-money is subject to its own rules that respond to its specific features. The EMR regulates the e-money product, setting out the prudential, issuance and redemption requirements, and defines e-money as a prepaid instrument. E-money is neither a deposit nor a debt instrument, and consequently attracts its own legal treatment. For instance, it can be purchased and sold, and is modelled on cash.

35. Furthermore, the e-money concept extends to distributed ledger products. As confirmed in the FCA's 2019 Guidance on Cryptoassets,[6] some distributed ledger technology ("**DLT**")-based tokens backed against a fiat currency (i.e. 'stablecoins') that meet the definition of e-money attract regulation as e-money. In the EU, the e-money concept extends to distributed ledger products set out in MiCA and will underpin the future digital euro proposition. We await further details of the UK government's future approach to the regulation of stablecoins, including on bringing the activities such as the issuance and redemption, as well as custody of fiat-backed stablecoins into the regulatory perimeter. To the extent that the government envisages developing (and reforming) the regulatory regime for e-money and the regulatory approach to stablecoins in parallel to create a regime covering both as products that differ primarily in the underlying technology (i.e. traditional e-money technologies versus blockchain), this would provide for another reason to keep e-money as a distinct product covered by specific rules responding to its specific features.

The attributes of e-money

36. E-money is an electronic surrogate for notes and coins[7], its issuance does not involve deposit taking, and users utilise it for making and accepting payments, receiving it in fulfilment of debt obligations.

    - E-money resides on electronic or magnetic storage systems/devices, usually of the issuer.

[6] https://www.fca.org.uk/publications/policy-statements/ps19-22-guidance-cryptoassets

[7] See Recital 13 to the second Electronic Money Directive 2009/110/EC ("EMD2"), and Recitals 3 and 7 of the first Electronic Money Directive 2000/46/EC ("EMD")

- It provides for a claim against the issuer for its exchange for bank money – the process of redemption. It is an electronic equivalent of a promissory note, like a bank note. It is a promise to pay, by the issuer, upon presentment, of the recorded value.
- A promissory note is an instrument in its own right, which can be transacted in and of itself. It can be transferred to others, and in so doing the rights associated with it are also transferred.
- In comparison, a deposit is a loan to the bank, and the depositor has a claim against the bank for repayment of the amount loaned. There are no instruments issued, and the claim must be enforced as a personal action by the depositor for repayment.

37. E-money is an innovation, an electronic equivalent of physical promissory notes, and has its own role in financial transactions. Bank issued notes (bank drafts) for example are commonly used as a means of payment, they can be accepted by third parties in fulfilment of debt obligations, with the recipient then seeking payment from the bank that issued the note. Cash is also such a note, but issued by the central bank. These exist side by side with other means of payment, including bank deposits.
38. The electronic money financial instrument can be purchased and sold as property, while also acting as a means of payment. The purchase and sale is however distinct from the use of the e-money in payment transactions.
39. The attributes of e-money mean that distribution of e-money can take place for example, without the distributor needing to be a payment services agent, as they simply buy and sell the e-money, without performing any payment services themselves. This is essential to the delivery of e-money products to users, and was, and continues to be, a key factor in the adoption and success of e-money.
40. When used as a means of payment, e-money is transferred as a category of funds within a payment transaction, and is accepted by payees in fulfilment of debt obligations.
41. Further, as a payment instrument, e-money can be given specific attributes that serve particular purposes: transfers can for example be made immutable, or free from defects in title such as may be desirable for low value payments; or alternatively subject to being reversed under certain conditions, combating fraud. Other arrangements have included separation of ownership rights from spending rights to enable restrictions to be imposed in corporate use environments. In such circumstances e-money may be made available to staff for expense management but the right of redemption is retained by the company.
42. The above attributes of e-money are embedded in the e-money industry, product propositions, contractual and distribution arrangements. The concept of e-money together with the regulatory treatment that responds to those features should therefore be preserved.

Summary

43. In summary:

- E-money is a district payment product and possesses legal attributes that enable its distribution without involving regulated payment services, facilitate innovation in formulating product propositions, and in solving business problems. The cost and impact of making any changes to the concept of e-money or its attributes would far outweigh the benefits that might be conceived.
- The EMA would support a more consistent approach to authorisation and regulatory permissions that allows regulated institutions that provide payment services to also issue electronic money, adopting the associated regulatory obligations, without having to seek an entirely different license.
- Further rationalisation of the EMR and the PSR in a single regulation could be appropriate, if there is a demonstrable benefit to it. For example, if it makes it easier for e-money firms to apply the rules relating to related and unrelated (to e-money) payment services.

Scope and definitions[8]

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

44. Generally, we consider the definitions and scope of the regulated activities captured by the e-money and payments services regime remain adequate, but would benefit from some improvements as outlined further in response to this Q3.

Regulated activities: general

45. We believe the description of some of the payment services listed in Schedule 1, paragraph 1 (Payment services) of the PSR could be reviewed to reflect more diverse products and services, namely:
    - Payment services listed as *execution of payment transactions covered by a credit line* (paragraph 1(d)) and *the issuance of payment instruments or acquiring of payment transactions* (paragraph 1(e)) make no mention of payment accounts. Where payment accounts are used in relation to such services, it has led to some ambiguity as to whether permission under paragraphs 1(a) or (b) must also be sought (as they include an explicit mention of payment accounts), even if no cash related services are offered. We believe that this would be an overly restrictive interpretation, and that permissions for payment services under paragraph 1(d) and (e) allow for payment accounts to be operated. We suggest adding the operation of payment accounts within permissions 1(d) and (e) to minimise this ambiguity.

Account information services ("AIS") and payment initiation services ("PIS")

[8] Parts 1 and 5, and Schedule 1 of the Payment Services Regulations, and Part 1 of the Electronic Money Regulations

46. We have a number of comments relating to the scope and definitions relating to AIS and PIS, as stated below. Further comments relating to the regulatory framework concerning these payment services are set out in response to Q8.

(1) Scope of AIS

47. 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.

48. We would welcome further clarification on the intention behind AIS and the broad scope of services which could be provided.
    - The current definition reflects the nature of AIS services at the time of drafting of PSD2, but today only reflects a small part of such services. We therefore consider it may be helpful to define AIS more broadly, for example, as services that involve authorised access to payment account data held by an account servicing payment service provider ("**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 accessing the account data; it would be disproportionate to regulate all of the parties that may be involved in the data flows.
    - 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 payment service users ("**PSUs**") via an interface (such as an app) developed and maintained by a third party technical service provider. It would be helpful to clarify that such third parties are not engaging in AIS when providing account information on behalf of the PSP with whom the account is held.

(2) "Accessible online" or "online access"

49. Regulation 69 and 70 PSR provide the right to make use of services of a payment initiation service provider ("**PISP**") or an account information service provider ("**AISP**"). The right does not apply where the payment account is not "accessible online". Article 31 of UK Regulatory Technical Standards on Strong Customer Authentication and Secure Communication ("**RTS on SCA**") requires that ASPSPs offering payment accounts that are "accessible online" provide a dedicated interface for third parties to access those accounts.

50. 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 ("**TPPs**") - 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."

(3) "Sensitive payment data"

51. Regulation 2(1) PSR defines "sensitive payment data" as data, as including personalised security credentials which can be used to carry out fraud. For the activities of PISPs and AISPs, the name of the account owner and the account number do not constitute sensitive payment data.

52. 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.

Payment account

53. 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 that flow from the holding of a payment account, particularly in relation to regulations 68-70 PSR on account access, and regulation 100(1)(a) in relation to the application of SCA, this is of key interpretative importance.

54. The Court of Justice of the European Union ("CJEU") case of *Bundeskammer für Arbeiter und Angestellte (Austria) v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG* has produced an unusual outcome, in that the PSD2 definition of a payment account is being interpreted by reference to the Payment Account Directive ("**PAD**"), rather than within PSD2 itself. The CJEU case suggests that accounts that are intended to be captured in PSD2 under access obligations set out at Articles 65-67 are informed by the definition at Article 1(6) of the PAD which require payment accounts to have a certain number of functionalities, which are: (a) placing funds in a payment account; (b) withdrawing cash from a payment account; (c) executing and receiving payment transactions, including credit transfers, to and from a third party. This relevant functionality that was utilised in the case related to the third functionality listed above (c) which provided for transfers to be possible to third parties. The FCA's guidance is informed by the outcome of this case, which includes at its Perimeter Guidance (PERG) 15.3, Q16 (What is a payment account?) that *"The possibility of making payment transactions to a third party from an account or of benefitting from such transactions carried out by a third party is one of the defining features of the concept of "payment account".* Whilst we are supportive of this criterion, and it has proven to be pragmatic, it is possible to suggest that other functionalities can also distinguish payment accounts. It would also be helpful for the definition of payment

accounts to be clarified within PSR itself. 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 scope, and for this to be set out in a pragmatic manner. Please also see further our response to Q8 (on accounts subject to access requirements).

Regulated activities and exempt/outsourced services

55. We would caution against proposals to extend the scope of the PSR/EMR regulatory regime to currently unregulated services, such as those of technical service providers or providers of other outsourced support services. Any such proposals would require careful consideration of their costs and benefits, the potential unintended consequences for the sector, as well as justification against the specific risks the proposed developments are intended to address.

56. PSPs leverage third party or intra-group outsourcing arrangements, the benefits of which often include greater speed to market, access to specialist resources, knowledge or technology, which PSPs would otherwise have to develop themselves. For example, in the intra-group context it enables PSPs to operate successfully within a global business, leveraging the technology owned or other resources provided by other group entities. For consumers, the benefits can in turn include more innovative, safer and/or cheaper products and services.

57. We believe there is a need for continued flexibility in utilising such third party or intra-group services; and that the existing outsourcing regime addresses the need for oversight and monitoring by PSPs of outsourced services. A proportionate and agile payment services regulation should balance the need to promote innovation and growth, and take into account the diversity of the business models across the sector. Regulating all service providers that provide technical or other services that support payment or e-money service would create inefficiencies, duplicating the costs of authorisation and compliance, and would have a disruptive effect on established and successful business models, which we submit would be out of proportion to the risks posed or the benefits to be achieved. We provide further comments as regards exemptions for technical service providers and intra-group services in response to Q3 below.

Cryptoassets (fiat-backed stablecoins)

58. We note that as part of this Call for Evidence, the government is considering *"[w]hether the definitions and scope of the regime are future-proofed for the rapidly changing payments and data landscape, including ensuring that the definitions are enabled for cryptoassets (including initially fiat referenced stablecoin –("**Stablecoin**")) where relevant"* (paragraph 20).

59. We expect the scope of the EMR and PSR regimes will be affected by the government's intention (as stated in HMT's Future Financial Services Regulatory Regime for Cryptoassets Consultation (February 2023)) to introduce a regulatory regime for Stablecoins which are used for payments. We understand that the regime will cover the activities of (i) issuance and redemption; (ii) custody; and (iii) payment related activities

for Stablecoins which are used in payments (paragraph 1.15 and Table 4A) ('Phase 1' regulated activities). Further, we understand the Stablecoin regime will involve making a range of specific amendments to the EMR and the PSR, to ensure it *"can be applied effectively"*, with further details of the government's approach to Stablecoins to be "*set out in due course*" (paragraph 3.14).

60. We await further details of the government's approach to bringing the 'Phase 1' Stablecoin activities within the regulatory perimeter. In this regard, we have the following comments to make.

61. In order to bring the EMR and PSR to bear on the issuance/redemption and payments activities undertaken using Stablecoins, the perimeter of these - or a future proposal, would of course need to be broadened accordingly.

62. Furthermore, while the objectives of these regulatory regimes continue to be relevant for Stablecoin products and services, the manner and focus of application will necessarily change. This is because distributed ledger technology ("**DLT**") necessarily impacts IT systems, governance, functions such as distribution, custody and customer relationships, and consequently the allocation of conduct of business and prudential regulatory obligations.

63. Issuance and redemption: just like e-money, Stablecoin issuers will be responsible for the issuance (including safeguarding) and redemption of value that they issue. The distributed ecosystem of DLT products however means that in most cases issuers will not have a day-to-day relationship with customers, and will rely on exchanges and custodians to facilitate the purchase of value that they issue and its onward sale to users. Similarly, when users wish to redeem value, they will rely on market intermediaries to buy the value in exchange for currency. The absence of a day-to-day relationship means that it is both more natural and more appropriate to consider the redemption obligation as one falling on intermediaries in the first place, and only where this fails being required to be met by the issuer.

64. A redemption requirement for Stablecoins should not however have an exclusive focus on the *direct* legal claim by the stablecoin holder against the issuer. Where there is a liquid market supported by the Stablecoin ecosystem and facilitating swift exchange for fiat currency, the ability of the user to satisfy their claim against the user facing entity (e.g. an exchange or other third-party intermediary) should suffice to meet a redemption requirement. It would be against the interest of consumers to require redemption directly and exclusively from the Stablecoin issuer, where such requests are readily fulfilled by third parties participating in the Stablecoin ecosystem. Furthermore, it may not be appropriate to impose equivalent legislative restrictions on the levels of redemption fees that may be charged in relation to Stablecoin redemptions. Where there are third parties involved in the value chain, the fee limitations could affect all of the parties throughout the chain, e.g. an exchange in a stablecoin exchange transaction. If the

compensation levels throughout the value chain were to be capped to the actual costs of redemption, for example, this could threaten the commercial viability of any such services.

65. Additionally, distributed ledger stablecoin products will have an architecture that separates the issuance of the token from the subsequent use of the token in a transaction, i.e. for payment activities. Once tokens are issued on a blockchain, the transaction process can be facilitated without any further intervention by the issuer. This can take at least two different forms:
    - One can be undertaken by individuals using their own private 'wallet' software. This impacts the scope of the issuer's powers and visibility over any use of stablecoins for transactions, consequently on any regulatory obligations or expectations placed on them in that regard. For example, this might mean that most of the equivalent requirements in the PSR, including as regards transparency, execution timeframes and/or liability for payment transactions will not apply to issuers, who have no control over such matters. It may be more appropriate to devise a more bespoke disclosure regime for stablecoin issuers, for example, that requires issuers to provide key information, such as the key features of the stablecoin product and the stabilisation mechanism used.
    - Alternatively, users may utilise the services of exchanges or custodians to undertake transactions within the systems of these crypto-asset service providers ("**CASPs**"), off-chain, in which case the transactions will bear a closer resemblance to familiar centralised payment systems than they do to DLT systems. For the purposes of such transactions, PSR related obligations may be more accessible to CASPs, being able to implement disclosure obligations and be held liable for proper execution of transactions etc.
66. Similarly, the separation between the issuance and transaction activities will have implications on the 3rd party service providers participating in the Stablecoin ecosystem. The extent and nature of the regulatory obligations and expectations placed on them will have to be calibrated to their respective roles and powers, the specific services they provide and the associated risks and means of mitigation.

67. Finally, we urge the government to ensure that the legislative process for the secondary legislation to bring the Stablecoin regulatory regime forward is subject to a considered consultation process. In particular, we expect such consultation and the future regulatory regime to acknowledge that fiat-backed stablecoin products and the parties involved in their issuance, redemption, custody and use for payments, have significant differences from those as envisaged by the current e-money and payment services regimes. For an agile and proportionate regulation, future fiat-backed Stablecoin regulation will need to consider and respond to the complexity and diversity of Stablecoin products, the different actors involved, their role in the underlying ecosystems and the specific services they provide.

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

68. We consider the exclusions under PSR and EMR remain appropriate and should be retained; however, some may benefit from revision. Below, we set out our comments on the negative scope/exclusions by reference to PSR Schedule 1, paragraph 2 (Activities which do not constitute payment services).

Limited network exclusion ("LNE") (paragraph 2(k)):

69. The scope of LNE services would benefit from a revision, with a view to broadening the types of activities eligible for LNE and improving the notification process.

70. The scope of LNE was significantly narrowed by PSD2, so as to apply only to payment instruments that can be used only in a 'limited way'. In practice, LNE typically applies to simple, limited use payment instruments, such as gift cards. In the context of payment instruments issued by professional issuers, the payment instruments are exempt under LNE if they satisfy one of the applicable conditions. Condition (ii) applies to payment instruments that allow the holder to acquire goods or services only within a limited network of service providers (merchants) that have *direct* commercial agreements with the issuer. The requirement for a direct agreement between the issuer and each merchant prevents contracting via, e.g. another entity within the issuer's or merchant's group, or contracting via a shopping centre where the merchants are located. This requirement is arbitrary; the limitations of the network where payment instruments can be used can be equally achieved via indirect contractual arrangements. We suggest this requirement for a direct agreement should be removed.

71. Further, there are payment instruments the acceptance of which is restricted, yet they are not excluded under LNE. The issuers of such products must therefore operate them as e-money products and be authorised as EMIs, with all the associated regulatory burden and costs that ensue. However, such products are more similar to limited network excluded products, and are not intended to compete with unrestricted use e-money products. We believe there is merit in revisiting the limitations imposed by the LNE conditions to take into account market practices, the way such products are used by consumers and consumer expectations with regards to such products.

72. LNE exempt product providers are subject to notification requirements to the FCA (regulation 38 PSR) when the conditions for notification are met (i.e. if the total value of payment transactions executed through relevant services exceeds EUR 1 million in the preceding 12 month period). Allowance for up-front notification should also be made to avoid the service providers having to terminate products, if they are interpreted by the FCA as not meeting the LNE conditions. The threshold trigger for notification should be increased (from EUR 1 million) to EUR 3 million to address increased use of non-cash products and inflation.

73. The FCA should be required to respond to the LNE notification with any objections it may have within a timeframe specified in statute, and if the FCA does not respond within this period, it should be deemed to have agreed to the service provider's notification. We believe a statutory timeframe of 2 months would be reasonable. This would reduce uncertainty faced by service providers following the submission of LNE notification.

74. Following the initial notification, no further notifications should be required unless there are changes to the service that impact the LNE notification - to reduce the administrative burden associated with the current requirement for annual re-notifications.

Electronic communications networks ("ECN") (paragraph 2(l)):

75. We support retaining this exclusion, and for the monetary limits pertaining to this exclusion increasing reasonably or with inflation. All parties in the chain should continue to benefit from the exclusion. For example, if the mobile network operator benefits from exclusion, other intermediaries for that transaction should also benefit from the exclusion.

Commercial agent exclusion ("CA") (paragraph 2(b)):

76. There is significant benefit in maintaining the commercial agent exclusion, as it allows for bill payments and similar arrangements to be offered. CA offers a cost-effective way to reach customers by allowing merchants to use commercial agents to negotiate and conclude contracts as well as collect payments, without increasing the risk to their customers. This can be particularly useful in entering new markets where commercial agents already have the infrastructure to help merchants (who may not have the same infrastructure) to offer their services/products, and the merchant can manage the risk in a similar way to other commercial risks. CA should be retained.

Technical service provider exclusion ("TSP") (paragraph 2(j)):

77. Retaining this exclusion from the payment services regulatory framework is of paramount importance. It provides for exclusion for technical service providers which provide IT support or similar, e.g. Software as a Service (SaaS) products for the provision of payment services. Regulated PSP remains responsible under the PSR for the provision of these outsourced "support" services.

78. Overregulation of TSPs would be detrimental to innovation and, ultimately, harm consumers and the economy. TSPs should be allowed to operate under an exclusion as they are subject to oversight by regulated entities.

Group company exclusion ("GCE") (paragraph 2(n)):

79. This is an important exclusion that should be retained. This incorporates a well-established commercial practice that reflects the fact that a group of companies is a single economic undertaking and that in many instances there will be a dedicated company providing treasury services to the other members of the group, without any intention of providing payment services as a business activity. Therefore, such activities should continue to be excluded from regulation.

Cash withdrawal services ("CWS") (paragraph 2(o)):

80. This exemption is helpful and enables independent ATM service providers to offer the technical facilities to enable cash withdrawals. At a time of increasingly sparse ATM coverage that is offered by the banking industry, and the ongoing policy challenge of

ensuring access to cash, this service is particularly important, and should be encouraged. Regulation of such providers as PIs would introduce complexity and cost that is not warranted.

Low-value exclusion:

81. In addition to existing exclusions discussed above, we believe there is merit in introducing a new exclusion for low-value payment instruments. In practice, such instruments are restricted in a similar way as LNE products, but they do not necessarily meet the LNE exclusion conditions. However, they are still restricted by their low value and as such pose a low risk.

The regulatory treatment of payment services and e-money[9]

Considered against the government's objectives for payments regulation (paragraph 14), and referring to paragraph 20 in the government's accompanying review document:

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

82. We consider the current authorisation framework for PIs and EMIs sets a high bar for regulatory supervision and does not require a reform. However, as noted in our response to Q2, we would welcome a more consistent approach to authorisation and regulatory permissions that allows regulated payment services firms to obtain permissions to issue electronic money, without having to seek an entirely different license.

Authorisation conditions generally

83. The PSD2 transposition significantly increased the requirements for authorisation of EMIs and PIs. Since then, further requirements have been introduced that further raised the bar and increased the resources required to obtain authorisation, such as the FCA's requirements on wind-down planning, operational resilience, and most recently, the Consumer Duty.

84. The changes in the FCA's policy on increased scrutiny on firms at authorisations gateway, coupled with FCA's staff and capacity shortages has meant that firms across the financial services sector have found it increasingly difficult to obtain authorisation, or have been invited to withdraw their applications, with limited opportunity to address the areas of concern to the FCA. The FCA's Authorisations Update of October 2022[10] shows that the number of firms (across the financial services sector) that were not authorised in 2021/22 was 1 in 5, up from 1 in 14 in the previous financial year. We consider this to be a reflection of not only the quality of the authorisation applications (which in some cases

[9] To note in particular, Parts 2, 3 and 4, and Schedules 2 and 3 of the Payment Services Regulations, and Parts 2,3 and 4 and Schedules 1 and 2, of the Electronic Money Regulations.

[10] https://www.fca.org.uk/news/statements/fca-authorisations-update

may indeed be lacking and should not be approved) but also a significant shift in the FCA's approach to authorisations, the influx of new applications from EEA-authorised firms who wish to continue to offer their services in the UK, the FCA's internal challenges of reviewing the applications within the statutory deadlines with limited resources, and thus limited opportunity to engage with the applicants.

85. Similarly, delays are experienced in the approval of change of control applications, negatively impacting the speed with which firms can raise investment in their business. We acknowledge the efforts and measures that the FCA has put in place, which are already leading to improvements in meeting its service levels. Nevertheless, the industry reports that the authorisation process has been excessively challenging, if not obstructive, and requiring significant investment of resources and time before the authorisation is obtained. The current 'road-blocking' approach will greatly inhibit the UK's ability to support new innovations in the industry and limit the provision of new services to UK based customers.

86. We would strongly urge the government to refrain from setting down further regulatory measures in the prudential and authorisations framework, which is already proportionate to the actual risk posed by e-money and payment services businesses to UK consumers or the UK financial system. Further enhanced authorisation requirements could limit the ability of new firms to become authorised, and existing firms to continue operations, thereby undermining the government's objectives for innovation, growth and competition.

87. We would however like to see an improvement in the requirements for authorisation/registration requirements for AISPs and PISPs to alleviate problems associated with obtaining the Professional Indemnity Insurance - see our comments in response to Q7.

Initial capital/own funds

88. Other than with respect to AIS and PIS services (see our response to Q7), we do not see the need to amend the initial capital requirements for authorised EMIs and PIs. However, we do see scope for improvement in the own funds requirements.

89. PIs are required to hold an amount of own funds that does not fall below the amount of initial capital or own funds calculated in accordance with Methods A, B or C, as the FCA may direct (regulation 22 and Schedule 3, paragraph 3 PSR). EMIs are subject to equivalent own funds requirements with respect to payment services that are not linked to the issuance of e-money (Schedule 2, paragraph 13(a) EMR). The three methods can give rise to significantly differing outcomes. The choice between turnover (Method B) and income (Method C) is particularly important and is subject to variations in business model and business practices (which may change over time). We therefore consider it important that both methods remain available to PIs (and EMIs) to adopt as appropriate.

90. 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. We suggest that the approach taken by the FCA should be based on consistent criteria (set out in legislation or secondary guidance) that are proportionate to the operational and financial risks faced by payment firms, and consider the relatively low risks that are posed by new firms (looking to establish their business and which have relatively small operations).

91. With respect to issuance of electronic money and related payment service activities, EMIs are required to hold the amount of own funds that does not fall below the required initial capital or an amount equal to 2% of the average outstanding electronic money of the authorised EMI (Method D) (regulation 19 and Schedule 2, paragraph 13(b) EMR). In order to ensure a consistent approach to capital requirements for PIs and EMIs, we would propose to consider a consistently calibrated scaling factor k (see Schedule 2, paragraph 21 and 22 EMR) for Method D. Since Method D is based upon average outstanding electronic money as a size indicator, it is effectively a proxy for operational risk. However, in contrast to both Method B and C it lacks the built-in digression by the decreasing scaling factor, and thus assumes a linear character of operational risk with increased e-money volumes, which we submit may not necessarily be the case.

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

92. We consider that the current registration regime for small PIs and small EMIs has operated effectively, and allowed smaller institutions to operate, scale up, and then apply for a full licence. It is a useful tool to allow market entry for new firms with limited available resources. It also provides a valuable option for firms whose e-money or payment service activities are limited in scale, for example, where they are incidental to the firm's other business activities. This regime furthers the government's objectives to support innovation and growth and is aligned with the risks posed by these small firms, and should be retained.

93. However, we consider that the volume caps for small EMIs and small PIs should be increased to remain in line with inflation for the next 5 years or so, and to reflect the continued need for innovation in this sector. Small EMIs are subject to a cap of the average outstanding e-money not exceeding EUR 5 million. For small PIs (and with regards to unrelated payment services provided by small EMIs) the average monthly payment transaction volume in a 12 month period must not exceed EUR 3 million. We consider an increase in the thresholds to EUR 6.5 million (from EUR 5 million) for small EMIs and EUR 4 million (from EUR 3 million) for payment services is reasonable.

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

94. Registration requirements for AISPs include a requirement to hold professional indemnity insurance or a comparable guarantee ("**PII**"). Similarly, this requirement applies to PISPs. However, TPPs have faced difficulties in obtaining suitable PII, hindering their access to the market. The EMA believes that it would be helpful to introduce initial capital requirements for both AISPs and PISPs **as an alternative to the PII for the purpose of authorisation.** TPPs could then be required to secure a PII without undue delay after being authorised. This also aligns with the European Banking Authority's proposals for improvements in this area in the future PSD3. Further, the requirements should afford TPPs flexibility to satisfy the requirements by either initial capital or PII/comparable guarantee option, or both, meaning that where initial capital is used to satisfy only part of the requirements, PII option could be used to satisfy the rest.

95. To increase the availability of suitable PII for TPPs, we consider the underwriting conditions, characteristics of the PII policies and the risks to be further clarified in order to resolve the market challenges. We would welcome the FCA undertaking such a review.

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

96. The regulatory framework for AISPs and PISPs has enabled new entrants to offer innovative services within this framework. This has, in turn, encouraged innovation, growth and competition. There have been, however, associated difficulties, which undermine these objectives and should be addressed.

Level-playing field for gaining AIS/PIS permissions

97. The restrictions on AIS and PIS permissions set out in the EMR and PSR distinguish the authorisation process for already authorised EMIs and PIs seeking to offer AIS and PIS services, from that for credit institutions (banks). In order to be able to offer these services, EMIs 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, in order to avoid giving an advantage in speed to market and service launch cost to credit institutions.

PIS framework

98. Regulation 69(3)(g) PSR provides that PISPs should not '*use, access, or store data*' for purposes other than the provision of PIS. This provision has introduced a constraint on the range of data available to PISPs for transaction risk analysis before initiating a payment, with the result that a PISP must have additional AIS permissions to access account data to assess the certainty of a payment being executed and to conduct fraud risk analysis. This is not only a barrier to market entry, but it limits the use of PIS in retail and e-commerce. PISPs should be able to access AIS data in order to manage their payment risk even if they do not intend to offer AIS products.

99. Regulation 69(2)(b) PSR provides the basis for ASPSPs to immediately provide the PISPs with "*.. all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction*". This means that if the ASPSP is not aware immediately after the receipt of the payment order whether the payment will be executed or not, it is not required to provide such information to the PISP at a later stage. Availability of accurate payment execution status is critical for PIS, particularly if it is to become a viable alternative payment type for retail payments (e-commerce or physical POS). We would encourage HMT to consider how the information flow between ASPSPs and PISPs can be improved e.g. potentially requiring ASPSP to provide the reason for decline/transaction failure (to the extent permitted by the proceeds of crime legislation) that would enable the PISP to assess whether transaction failure was due to fraud, or another reason (e.g., an authorisation issue). This would also enable PISPs to assist with fraud prevention.

AIS framework

100. Regulation 70(3)(d) PSR provides that AISPs must not "*access … information other than information from designated payment accounts and associated payment transactions*". This has led to broad interpretation by ASPSPs and varying datasets being made available to AISPs, thus limiting AISPs' ability to provide consumers and businesses with comprehensive services envisaged by the regulations by reinforcing the informational imbalance between ASPSPs and AISPs. In order to level the playing field between all parties offering AIS services, we suggest that this provision is updated to clarify the scope of payment account information to be provided to AISPs, and ensure that AISPs can access all data on a payment account.

101. Data parity between ASPSP's online channels and data accessible to AISPs is not adequate; all payment account data must be made available. In order to achieve this, it may also be necessary to further explain the definition and scope of 'sensitive payment data' to facilitate a common understanding of the data elements to be made available (see our response to Q3 above).

Accounts subject to TPP access requirements

102. A blanket requirement to provide access to all payment accounts held by ASPSPs has resulted in unintended consequences. ASPSPs have faced significant costs in developing compliant access interfaces to payment accounts. This has had particular impact on smaller ASPSPs who, as yet, have not seen significant 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. The access requirement can also be a barrier to entry for small and niche innovative financial solutions.

103. We therefore consider that there is an opportunity to introduce thresholds (volume of payment accounts, of transactions etc.) below which ASPSPs could operate payment services 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 see no demand from TPPs for access.

APIs and standardisation

104. We consider that further alignment on industry API open banking standards will help to mitigate against implementation complexity and cost. In particular, when considering payment initiation APIs, there are a number of areas where further standardisation would assist PSPs to develop innovative PIS solutions. However, legislating for a common PSR API standard risks the technical neutrality of the regulatory framework, which in turn may limit the opportunity for market innovation. It also does not consider the experience from implementing existing Open Banking Implementation Entity standards in the UK whereby the use of a common API standard has not resulted in common interpretation of the standards, nor consistent API performance and availability across ASPSPs.

105. Nonetheless, whilst TPPs have to navigate a complex ecosystem to maintain access to multiple payment account interfaces, a thriving market of intermediary API platforms providers (who manage the complexity of API fragmentation) has emerged as a direct result of the requirements of the PSR. Hence, we do not consider it necessary for a legislative solution for common API standards. The open banking ecosystem could be improved if the PSR requirements for a dedicated interface are further supported by robust guidance on the availability and performance of the interface within secondary legislation provided by the regulators.

Open Finance

106. We consider that if compelling customer-driven propositions can develop that encourage data providers to facilitate standardised, high-quality access to data, competition and innovation benefits of the PSR will be increased. The investment made by providers of payment accounts to support real-time networked access to account data has been substantial. Therefore, any expansion of the open banking framework should be carefully considered against customer requirements and expected benefits, so that incentives can align and the cost of upgrading infrastructure to allow access to data is focused where there is likely to be significant market demand.

107. We also suggest that it would be disproportionate to require AISPs registered under the PSR to access payment data, to also comply with an additional open finance registration regime in order to be able to access a wider set of financial data sets when they become accessible.

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

108. We consider the current agent registration regime has been effective and does not require a reform.

Information requirements for payment services[11]

Considered against the government's objectives for payments regulation:

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

109. Part 6 and Schedule 4 PSR requires specific disclosures to payment service users ("**PSUs**") relating to the PSP, the transactions, and to liability and dispute resolution. We consider the prior information required before the conclusion of a single payment service contract (as required under regulation 43 PSR) or before entering into a framework contract (as required by regulation 48 PSR) is sufficiently extensive. Note that the information required under PSR is not the only information that must be supplied in relation to payment services. For example, the Financial Services (Distance Marketing) Regulations 2004 sets out information that must be provided to consumers before entering a payment services contract concluded at a distance. We comment further on the additional information required under the Cross-Border Payments Regulation in response to Q11. Ultimately, PSUs are provided with a considerable amount of information before and after they enter into a contract with the PSP and/or make a payment. These requirements are significant in volume and do not merely arise from the PSR. We consider the introduction of any further information requirements could be counter-productive, increasing consumer confusion and fatigue over voluminous disclosures. We would urge the government to refrain from introducing additional information requirements.

110. However, we would welcome improvements in the information requirements in the areas set out below.

- **Consolidation:** We would welcome consolidation and rationalisation of the information requirements set out in various legislative instruments, to make it easier for PSPs to navigate, reducing compliance costs.
- **The means for providing information:** Generally, PSPs are required to provide or make available information mandated under PSR on paper or durable medium (see regulation 55(1) PSR). We consider these requirements would benefit from a revision with a view to affording PSPs more flexibility on the means by which the required information is provided to their customers, to reflect current consumer practices and expectations, in line with the principle for more agile regulation. For example, providing the information through an app or a dedicated online interface (e.g. online account) should be sufficient to meet the regulatory requirement to provide the information on a durable medium, even if the customer has to log in to view it. PSPs should be free to determine the customer communication channel used, to be able to adapt to the information needs and expectations of their customers.

[11] See in particular Part 6, and Schedule 4 of the Payment Services Regulations

Low-value payment instruments (regulation 42 PSR):

111. The current low-value payment instrument value limits are too low, meaning that PSPs are seldom able to utilise the simplified information framework provided for under regulation 42. This is disproportionate, considering the simplified information framework was intended and should be available for simple, low value payment instruments. The values under regulation 42 should be increased to reflect inflation and utility of instruments. We consider an increase in value to EUR 100 for individual transactions (regulation 42(1)(a)), spending limits to EUR 500 (regulation 42(1)(b)), and storage limits to EUR 1,000 (regulation 42(1)(c)) to be reasonable.

Micro-enterprises (regulation 40(7) PSR):

112. Whereas a simplified framework is available as regards (large) corporate customers, PSP's customers that are micro-enterprises are treated the same as consumers for the purposes of the PSR information requirements. We consider this homogenous treatment of micro-enterprises as consumers for the purposes of PSRs is problematic and would benefit from revision. Where the PSP's customer base consists of companies that include large corporate customers as well as micro-enterprises, it is difficult and resource intensive for PSPs to identify and delineate between micro-enterprises and other corporate customers. Accordingly, PSPs tend to err on the side of caution and apply the PSRs information requirements to a broader range of entities than required under the PSRs, resulting in a greater regulatory burden than envisaged under the regulations. It would be much easier and therefore efficient to differentiate between individual and business customers. We therefore suggest that regulation 40(7) would benefit from revision to remove the mention of micro-enterprises. The revised regime could continue to include individual business customers, such as sole traders, to benefit from treatment as consumers. We submit further comments in relation to the rights and obligations under PSR concerning micro-enterprises and other corporate customers in response to Q24.

113. In scenarios where a service offered to a payer by a merchant is facilitated by a PISP acting on behalf of the payee, we do not believe any additional disclosure obligations are required in legislation. There are instances where a number of service providers may be involved in delivering a payment service to the customer (whether it is the payer or the payee); and different arrangements result in different contracting parties. In such instances, the customer should be able to clearly discern the parties with whom the customer is contracting from their framework or single transaction contract.

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

114. The EMA would welcome changes to the Cross-Border Payments Regulation ("**CBPR**") requirements detailed below.

Consolidation of CBPR within PSR

115. CBPR transparency requirements apply to PSPs and parties providing currency conversion services at ATMs or the point of sale, supplementing and cross-referencing the information requirements under PSRs that apply to them. We consider it would be beneficial to consolidate the CBPR requirements within the PSR, to ensure better coherence and alignment of the information requirements. Such consolidation should also remedy the CBPR text inconsistencies detailed below.

116. We also believe that provisions relating to FX fees could be alternatively set out as total costs to users of making transactions, enabling more direct comparisons to be made in the same way as an APR is used for credit.

Remedy the CBPR text inconsistencies

117. The CBPR text, as retained in the UK law, has inherited some inconsistencies and ambiguities that would benefit from remediation. These are:

- It is understood that Article 3a CBPR requirements only apply with regards to information currency conversion charges related to **card-based transactions**. However, there is no definition of the term 'card-based transaction' provided in the CBPR (or, in fact, in the PSR) – this term is only used in the heading and not in the text of Article 3a CBPR. In the absence of a definition, the term has been interpreted in light of the definition of the term in the Interchange Fees Regulation, i.e. as including credit card, debit card and prepaid card transactions based on payment card scheme's infrastructure. It is suggested that Article 3a CBPR would benefit from further clarification to confirm its applicability to 'card-based transactions', defined in line with the definitions used in the Interchange Fees Regulation;

- The applicability of disclosures required under Articles 3a and 3b with regards to **customers other than consumers** has been subject to some ambiguity as they were introduced. Both Articles 3a and 3b of UK CBPR make a reference to ('*with regard to*') information requirements set out in Part 6 of the PSR (regulations 43(1), 48(1) (taken with paragraph 3 in Schedule 4 PSR) and regulation 57(2)). Regulation 40(7) PSR allows PSPs and their customers to agree that any or all of the information requirements under Part 6 PSR do not apply (except where a PSU is a consumer, a micro-enterprise or a charity (as defined in the PSR) - this is known as a 'corporate opt-out'. The broadly held view is that the transparency requirements under Articles 3a and 3b CBPR clarify and are therefore subject to the scope of the general disclosure obligations under PSR, meaning that if a PSP has agreed to a corporate opt-out from the information requirements with its customers in accordance with the PSR, the transparency requirements under CBPR equally do not apply. We agree with this view and consider it to be consistent with the intended purpose of the CBPR transparency requirements; however, we consider an additional clarification to this effect may be useful. The consolidation of CBPR requirements within PSR could easily achieve this.

- Non-applicability of Articles 3a(5) and 3a(6) CBPR. The EU CBPR Articles 3a(5) and (6) (on electronic messaging on currency conversion mark-ups) became applicable from 21 April 2021, i.e. after the end of the transition period applicable to the UK's

withdrawal from the EU and therefore could not be onshored into UK law under the terms of the European Union (Withdrawal Act) 2018 (as amended). The UK government confirmed that Articles 3a(5) and (6) will not come into UK law in its Explanatory Memorandum (paragraph 2.69) to the Securities Financing Transactions, Securitisation and Miscellaneous Amendments (EU Exit) Regulations 2020/1385. However, regulation 72 of these Regulations did not specifically amend the EU CBPR text so as to remove Articles 3a(5) and 3a(6). It is understood that such an amendment was deemed unnecessary as Articles 3a(5) and (6) could not form part of the retained EU law. Nevertheless, it may be beneficial to additionally clarify that these requirements do not apply in the UK, to avoid any confusion.

Rights and obligations in relation to the provision of payment services[12]

Considered against the government's objectives for payments regulation:

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

118. The EMA considers that the framework for termination of payment services contracts established under PSR achieves appropriate balance between the rights and obligations of PSUs and their PSPs.

119. The regulatory framework concerning payment services contract termination are already weighted in the PSU favour, affording appropriate PSU protection. This includes:

- a requirement to provide at least 2 months' notice to terminate a payment services contract concluded for an indefinite period, where a contract so provides (regulation 51(4) PSR); further PSU protections are prescribed as regards their ability to terminate the contracts and termination charges.
- any consumer contracts, including payment service contracts, are subject to further requirements regarding transparency and fairness of the contractual terms, including on termination, under the Consumer Rights Act 2015 ("**CRA**").
- PSUs (including consumers, micro-enterprises and small businesses) who have complaints about access to their services terminated, also have the ability to have their complaints reviewed by the Financial Ombudsman Service;

[12] Part 7 of the Payment Services Regulations

- FCA's Principles, notably Principle 6 (having regard to customer's interests and treating them fairly) and Principle 7 (fair, clear and not misleading communications) apply to PSP's relationships with its PSUs;
- The Consumer Duty rules, affording higher standards of protection of PSU's interests on all aspects of their use of or interactions with the PSP's retail business.

120. Accordingly, the existing regulatory PSU protections already place significant restrictions on termination of payment service contracts by PSPs. The existing rules provide for a framework that appropriately balances the PSP's and PSU's interests around service provision and its termination. Termination by PSPs generally, results from an underlying issue associated with the PSU's use of the product or service, such as abusive or damaging behaviour. PSPs have a legitimate interest in protecting their business and should be able to exit the relationship with their PSU, in the event that their services are abused by PSUs. The regulatory protections under the PSR, CRA and the FCA's rules ensure that the termination rights are balanced and exercised in a considered manner by PSPs. At the same time, the PSUs' interests are protected, as they are free to terminate their payment services, usually immediately in accordance with the industry practice, and in any case with not longer than one month's notice. The financial and business impact on making changes to this framework would be significant, and therefore could be out of proportion to any benefits to be achieved.

121. Finally, PSPs contracting with certain large corporate customers (i.e. not micro-enterprises) are able to agree different terms, including as regards termination and the notice period, in accordance with regulations 40(7) and 63(5) PSR. It is very important that this provision is retained to allow for the freedom of contract between two commercial parties, and the management of risks between them just like any other commercial and business risks.

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

• that, as a general principle, a notice period and fair and open communication with a customer must apply before payment services are terminated?

• that the regulations and wider law operate here as set out under paragraph 29?

122. A notice period and fair and open communication with customers before termination of payment services can act as a general principle, and we consider this to already be the case under general consumer protection law and the FCA's principles.

123. However our members do note that the reasons for termination are wide-ranging; a PSP must be able to determine how their services are used in order to effectively manage the risk to their business. This means that there may be circumstances other than suspected or actual criminal offences (where determining criminality of the conduct is a complex matter in itself) where PSPs may have to and should be allowed to terminate the customer relationship sooner; this may equally affect the appropriate communication

with customers regarding termination - see further our response to Q14. For example, PSPs may not wish for their products to be used with certain categories of merchant (e.g. gambling services), and this may be a business development that takes place later in the business relationship with the PSP's client. The PSP may have a legitimate interest to terminate such relationships with immediate notice, considering the damage this may have in to the PSP's relationships with other regulators or partners, such as payment systems and the card schemes.

124. We agree the regulations and wider law operate as set out in paragraph 29 of this Review and Call for Evidence. However, we have an important point to make: for the reasons discussed above, PSPs may wish to exit the relationship with the PSU, with immediate notice, for example, where necessary to manage the damage arising from PSU's continued use of the service – it should be acknowledged that PSPs are and should be able to do so, as and when permitted under the current regulatory framework.

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

125. PSPs should be able to set their own risk appetite and to determine how their products and services can be used. Managing the customer expectations and permitted behaviour via contractual means is an important tool; it enables PSPs to ensure that their regulatory and other legal obligations, such as to the PSP's partners or payment systems, can be met. Similarly, exiting the customer relationship is a necessary tool to enable PSPs to manage risks to their business.

126. PSPs may need to terminate contracts with their users for a variety of reasons. These include replacing their products with new and improved product offerings or withdrawing unprofitable ones. PSPs may also have to cease doing business with customers for financial crime reasons, for example, if a customer is engaging in illegal activities, or fails to provide information (or provides false information) required for meeting customer due diligence requirements. Further reasons include where the customers activities and/or use of the services fall outside of the PSP's risk appetite, eligibility criteria or permitted use of their services or where necessary to meet PSPs contractual and legal obligations to payment systems (including card schemes such as Visa, Mastercard).

127. Without commenting on when notice periods are or are not applied, we consider that there are circumstances where a PSP may have to terminate the relationship with their customer sooner, and that they should be able to do so. This includes actual or suspected criminal activity, but could also apply to the use of services for activities that are not necessarily illegal in the UK (but can be in other jurisdictions) or are otherwise prohibited by the PSP, in order to manage compliance with the PSP's risk appetite and necessity to meet the PSP's regulatory and other contractual obligations. The fallout from the PSP allowing such activities to continue can be grave, resulting in adverse regulatory action, fines, loss of core business partners etc; PSPs must be able to manage such risks, as expected of a prudent and responsible provider. However, this does not mean that the PSU's interests are not considered or protected on termination under

the current regulatory regime. For example, terms in PSP contracts with consumers, including termination terms, continue to be subject to the fairness requirements under the CRA and the FCA's Principle 6 requires PSPs to treat their customers fairly.

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

128. The EMA considers the current requirements under regulations 51 (on termination of payment services contracts) and 71 (on the right to stop the use of payment instruments) PSR are effective. They already provide for important safeguards and requirements for customer notification. In the case of termination of payment service contracts concluded for an indefinite period by a PSP, this includes a requirement that at least 2 months' notice of termination is given (regulation 51(4) PSR).

129. In the case PSP's right to stop the payment instrument, this applies on reasonable grounds relating to (a) the security of the payment instrument, (b) suspected unauthorised or fraudulent use, and (c) increased risk of non-payment (for instruments with a credit line) (regulation 71(2) PSR). The customer's prior notification requirements under regulation 71 are qualified to allow PSPs notifying the customer *immediately after* where prior notification is not possible and no notification is required where it would compromise reasonable security measures or would otherwise be unlawful. These are important qualifications that acknowledge that PSPs may have to stop payment instruments immediately, without prior notification, to prevent fraudulent use and further losses as well as that PSP's other legal obligations may prevent customer notification (where it would be unlawful). We consider these requirements are effective, including on customer notification requirements, allowing for a variety of reasons and actions which should be taken by PSPs, depending on the reasons that lead to stopping of the PSU's payment instrument.

130. We note that the FCA's Principles, notably Principle 6 (having regard to customer's interests and treating them fairly) and Principle 7 (fair, clear and not misleading communications), also apply to PSPs, including in relation to notices and communications provided for under regulations 51 and 71 PSR. These principles and requirements are being further supplemented by the Consumer Duty rules. Accordingly, we consider that the existing regulations are effective and sufficient in ensuring that the termination notices are given and that the communications are clear and fair, in accordance with the applicable rules.

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

131. We consider the existing PSU protections against the termination of payment service contracts are sufficient, and no additional protections are needed. PSUs who have

concerns regarding their freedom of expression are already subject to all of the protections that apply to any user, including under the PSR, the FCA's rules, the consumer laws and the Equality Act 2010.

132. As stated in response to Q12, the existing PSU protections already place significant restrictions on termination of payment service contracts by PSPs, including a requirement for the PSP to provide at least 2 months' notice to terminate contracts of indefinite duration. This is a well-established framework that balances the PSP's and PSU's interests around service provision and its termination. PSUs (including consumers, micro-enterprises and small businesses) who have complaints about access to their services terminated, also have the ability to have their complaints reviewed by the Financial Ombudsman Service. PSPs have a legitimate interest in protecting their business and any additional PSU protections in this area should not come at the expense of those interests.

133. The financial and business impact of introducing additional PSU protections in this area would be disproportionate and damaging to PSP's ability to manage their business risks and liability effectively, as well as curtailing their freedom to conduct business. Contract termination is an important tool for managing the damage and risk to the PSP's business that arise from a customer relationship. Inability to exit the customer relationship, including by having longer termination notice periods, can reduce the speed with which customers can be migrated to better products, expose the PSP to adverse regulatory action or penalties from payment systems, as well as liability to other suppliers throughout the payments ecosystem. PSPs should be able to set the risk appetite for their products and services and to use the contractual tools for managing their risk. Accordingly, the EMA considers that the impact of imposing any additional PSU protections, including longer termination notice periods, would be disproportionate and damaging to the payments sector.

134. We envisage many conceptual and practical issues associated with any additional measures placed on PSPs regarding or preventing termination of contracts to protect the PSU's freedom of expression. There are:

- **Unfair to single out payments sector:** We consider it would not be equitable to hold the payments sector to a higher standard when compared to other industry sectors. It will impose an additional regulatory burden and costs of payment services firms. Ultimately, it would be damaging to the competitiveness of the payments sector, as well as to the international competitiveness of the UK economy.
- **Inappropriate regulation on human rights issues:** PSR regulate the provision of payment services on matters such as service levels and security of payments, and the rights and obligations of both the PSP and the PSU pertaining to payment services. PSUs who have a complaint about their PSP, including, for example, the termination of their services, have the ability to refer their complaints to the Financial Ombudsman Service. Complaints about PSPs who fail to meet their obligations under PSR can also be raised with the FCA, as the responsible regulator. PSR is not an appropriate legislative mechanism with which to regulate on matters relating to human rights

issues, including the freedom of expression. Nor would it be appropriate for the Financial Ombudsman Service or the FCA to become adjudicators on such issues. As a financial services ombudsman and regulator respectively, neither is likely to have the required expertise to deal with alleged violations of freedom of expression or any other human rights, which in themselves are likely to involve a complex set of legal issues.

- **No supporting framework:** Imposing any additional obligations on PSPs concerning their PSUs' freedom of expression will force PSPs to make difficult determinations on complex legal issues. For example, how should the payments industry distinguish between "free speech", "hate speech" and criminal incitement? Would the UK government provide guidance and safe harbours? A regulation which is not supported by a thorough analysis of its impact and appropriate guidance risks leading to unintended outcomes.

135. We have not seen evidence of PSPs engaging in "cancellation" practices, i.e. terminating PSU contracts due to the views expressed by PSUs. The Review and Call for Evidence refers to anecdotal evidence - a "perception" - of the reason for termination of contracts in the cases referred to in the Review. In line with the government's objectives for payment services regulation outlined in this Review and Call for Evidence, and considering the broad and damaging consequences any changes could have on the payments sector, we expect the government to ensure that real evidence is used to substantiate any proposals for a change in this area of law.

Wider considerations in relation to the provision of payment services

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

136. Regulation 66(2) PSR prescribes a SHARE arrangement on fees, whereby the payer and the payee must each pay their respective PSP any relevant fees. We consider it may be beneficial to remove this provision, thus allowing for new products and services to evolve by offering flexibility to PSPs in adopting different fee sharing arrangements. Recital 65 of PSD2 provides that the SHARE provision was included merely for efficiency. We consider that the removal of this provision would allow for the evolution of products and services that were not anticipated when PSD2 was brought into force.

137. However, any changes to the SHARE provisions should only be made to the extent they do not impact the UK's ability to continue to participate in the SEPA framework. Accordingly, it may be necessary to retain the SHARE rule in regulation 66(2A), which deals with SEPA transactions, and to agree to any changes to the requirements on charges with the Eurosystem, and with the European Payments Council.

138. Further, the removal of SHARE requirement should not prejudice PSPs' ability to comply with any fee rules pertaining to any other payment systems through which transactions are affected.

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

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

Sending and receiving PSPs

139. Broadly, the EMA considers that the framework established under PSRs for the rights and obligations of sending and receiving PSPs remains appropriate. PSPs are familiar with this framework and have it built into their operations as well as commercial relationships. Any changes to the framework will likely cause significant disruption and costs to PSPs having to adjust. In particular, any changes in the liability framework could have a significant disruptive effect, eradicating the profitability of existing payment products and/or competitiveness of any new or innovative products.

140. The EMA is aware that the overall framework of the rights and obligations between sending and receiving PSPs is being shaped by other policy and industry initiatives, for example the ongoing proposals on the PSP reimbursement of APP scam victims. As this framework is evolving, the EMA considers it inappropriate to make further legislative changes at this time.

ASPSPs and TPPs

141. We are aware that some consumer groups and ASPSPs would like to revisit the rights and obligations for AIS and PIS providers in the PSRs.

142. With regards to payments, the EMA considers there is scope for a multilateral framework which addresses the rights and obligations of market participants in order to drive forward Open Banking payments, particularly for commercial Variable Repeat Payments (VRP). However, we believe any framework should be market driven, and not as a result of a legislative change to the PSRs.

143. In relation to AIS, we consider that any changes to the rights and obligations to the PSRs should only be made when a clear legislative framework for Open Finance is available.

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

144. The EMA considers that tackling fraud requires a combined effort from all the actors involved. Fraud is ever evolving, and measures targeting solely PSPs are unlikely to be effective. PSPs already have incentives to combat fraud, therefore legislating in PSR or similar legislation that targets PSPs would not be appropriate.

145. With regards to the government's current approach to legislate in the Financial Services and Markets Bill, directing the Payment Systems Regulator to require PSPs to reimburse their customers for loss sustained from authorised push payment ("**APP**") scams, the

EMA believes this approach is flawed and will come at the expense of the government's objectives for growth, innovation and competitiveness in the payments sector. We elaborate on the reasoning for the EMA's views below.

Inadequacy of general anti-fraud measures targeted at PSPs

146. Fraud is ever evolving and it is not solely a payments sector issue; combating fraud requires a combined effort from all the actors involved. PSPs will keep implementing new processes and tools to identify and stop fraud, and consumers should keep being educated and warned on the emerging fraud typologies. Raising awareness of the risks of fraud is one of the most effective tools to prevent fraud in the long term, preventing fraudsters from being able to shift towards new typologies when the old ones become too well-known to be efficient. Additionally, other actors should be encouraged to participate more actively in combating fraud, for example in relation to social engineering fraud that makes use of social media platforms, or telecommunications providers. We welcome the introduction of the Online Safety Bill, which we hope will alleviate some of the problems associated with fraudulent advertising, but we consider that more could be done cross-industry.

147. PSPs are already implementing effective measures against fraud, based on the specific typologies of fraud encountered by different PSPs, and adapted to their own business models. Measures to combat fraud are only efficient when perfectly tailored to the PSP's needs, and when they are based on the knowledge of the PSP on its own fraud risks and of the current and emerging fraud typologies that may impact its clients. Therefore, general additional measures against fraud threats in payments are not necessary or even advisable.

148. Anti-fraud measures prescribed in payment services legislation also run the risk of simply shifting the fraud elsewhere, as criminals adjust to seek out new opportunities. We see evidence of this from the introduction of SCA, where the fraud rates for unauthorised transactions have decreased (albeit at the cost of significantly reducing successful completion of transactions). At the same time, EMA members have witnessed a migration towards manipulation of the payer (APP) fraud, which SCA does not address. The EMA therefore believes that focusing on types of fraud, particularly by legislative measures, may not be effective overall.

PSP reimbursement of APP scams

149. We fully appreciate the magnitude of the concerns around APP fraud, and in particular the growing nature of this form of fraud, which was exacerbated by COVID-19. We recognise the heavy losses incurred by victims of APP fraud, not only in monetary terms, but also in terms of emotional and psychological damage.

150. We note the government's intention to legislate via the Financial Services and Markets Bill directing the Payment Systems Regulator to require PSPs to reimburse their customers for APP scam losses. Whilst we acknowledge the political context of these proposals, the EMA is concerned about the potential impact on the UK's payments and fintech industry.

151. We have put forward principled arguments against the proposals to hold PSPs liable for loss incurred by payment service users arising from APP scam throughout the evolution of these proposals. To date, our arguments have not been refuted nor appropriately addressed. We therefore find it necessary to repeat them, and urge the government to consider them, against the government's stated objectives in this Review and Call for Evidence for payment service regulations that include proportionate regulation, innovation, growth and competition in the payments sector as well as appropriate protection for consumers.

152. We consider that placing liability on PSPs for losses incurred by victims of APP scams, as per current proposals, is inappropriate for the reasons outlined below.

(1) Incentivises fraud

153. PSPs' underwriting of customers' APP scam losses will create a moral hazard and increase the likelihood of first-party fraud. So far no evidence has been provided to the contrary. This would defeat the government's overall objective of reducing APP scams by creating a favourable environment for payment service users to engage in a different type of fraud (i.e. fraud perpetrated by the payer rather than the payee).

154. Directing PSPs to reimburse customers for APP fraud will incentivise criminals from outside the UK to target the UK because customers need not be careful because they know they will be reimbursed in any case. In other words, **the UK will offer easy money to criminals** in comparison to other countries that do not have a reimbursement requirement. We run the risk of the UK being viewed (to an even further extent than at present) as an "easy target" in comparison to other countries. The UK is already singled out as a target to perpetuate scams - one EMA member provided data showing that whilst the UK represents 20% of their customer base, it gives rise to over 60% of their APP fraud cases. The data illustrates that the UK is clearly singled-out as a target for APP scammers, and we consider that more available money would more likely increase – rather than reduce - instances of APP fraud.

(2) No liability where PSPs are not at fault

155. We consider it to be disproportionate to levy liability on PSPs for loss arising from an APP scam when a PSP is not at fault. There is a clear distinction between compensation that is triggered by PSPs failing to meet a duty of care, which is appropriate, and one that amounts to an insurance scheme for all APP scam fraud.

156. Please note that under principles of English law, a PSP would not be liable to a customer for this type of loss; for that reason, we disagree with any proposal for mandatory reimbursement.

Impact on Faster Payments Scheme ("FPS")

(1) Increased cost

157. Mandatory reimbursement will result in an increase in the cost of using FPS, which will be borne by PSPs and will ultimately be passed to consumers.

158. Applying mandatory reimbursement through the FPS rules also removes the ability to set a standard of care for consumers, and moves more directly towards a complete underwriting of fraud by the PSP industry. It is also not in the interests of users, whether consumers or businesses, to address fraud risk through underwriting; it simply shifts the cost of the fraud back to users who will have to pay through higher fees, and fails to address the vulnerabilities in the ecosystem that give rise to the fraud in the first place.

(2) Hampering competition

159. Imposing the cost of compensating victims of APP scams directly through the FPS is anti-competitive because it favours incumbent institutions with a large customer base. This is because a larger proportion of their customers' payments will be routed within the bank's own payment network and therefore will not be subject to FPS rules. For example, one entity claims to have a market share for current accounts of approximately 20-25%. In effect, this means that when a customer of this entity makes a FPS payment, there is a 1 in 4 chance that they will not be subject to the FPS scheme rules (because it could be an internal network transfer to another account held at that institution).

160. This will result in specialist PSP products becoming less competitive, when in fact their entire business is predicated on creating more efficient and cheaper products than incumbent PSPs and banks. The increased cost of covering possible fraud liabilities may also create a significant barrier to entry for PSPs seeking to participate in the FPS scheme.

(3) Impact on payment specialist PSPs

161. PSPs who are members of the EMA are principally specialist payment providers who are proscribed from lending the funds of users, and therefore are restricted in the income that they generate to transaction related income streams. The impact of any increase in cost is felt much more by these PSPs (i.e. non-bank PSPs), as they do not benefit from the cross-subsidisation afforded by banks. Whilst they may be able to put in place technical and operational measures that reduce the risk that their customers might suffer from APP scams, it is much harder for them to absorb the cost of an APP scam, or the cost increase of FPS scheme fees.

162. As an example, if the total revenue generated by a PSP was in the region of 1% of the value of a transaction, from which its cost of doing business must be extracted, it would have to process at least 100 equivalent size transaction to recover the loss on a single claim of fraud. Once the costs of doing business are taken into account, this is likely to increase to perhaps 1000 or more transactions.

(4) Impact of organised criminal activity

163. APP scams can be operated by highly sophisticated organised criminal groups that specifically and aggressively target a particular group of users (this happens by analogy to different types of PSP). As such small and market entrant PSPs could be effectively driven out of business due to compensation payable in relation to quite a short period of time during which the PSP mitigates the specific targeting and prevents further APP scams.

164. This can happen irrespective of the strength of controls in place as organized crime groups can be highly innovative. The pattern is then that the APP scam migrates to another user group that may be attached to another PSP. Non-bank PSPs are far less able to cope with the compensation relating to such targeting APP scams than banks due to their business models and length of trading during which reserves are built up.

(5) Impact on Open Banking & competition with card payments

165. If FPS places liability on direct participants for reimbursement of APP scams, then participants may well look for opportunities to shift liability to other PSPs in the payment chain wherever they can. Increased fraud liability, coupled with increased operating cost, may make some innovative PSP business models, such as payment initiation service providers (PISP), commercially unviable. PISPs typically do not enter into the flow of funds of the payment transactions they initiate, thus limiting their capacity to offset increased fraud liabilities which may be incurred.

166. It is therefore crucial that a sensible balance is struck between protection for customers where the PSP has failed in their duty of care, and where an individual has authorised a payment, with all possible information provided and support offered by the PSP.

(6) Impact on indirect participants

167. The impact on indirect members is very unclear, as changes to FPS rules do not usually include instructions on the cost when passed to indirect members. EMA members range in size, with several processing FPS volumes in excess of several million transactions per annum, and there is no guarantee that sponsor institutions will choose not to pass on the increased cost of FPS on to those PSPs.

168. Most indirect PSPs have limited influence over FPS rules. Equally, third party payment (TPP) providers have similarly minimal influence over any changes to the FPS rules.

169. Ultimately, we consider the reimbursement requirement is not well thought through – it will result in fraudsters specifically targeting the UK over other countries for easy money and will have severe adverse consequences for the payments industry, undermining the government's objectives for innovation, growth and competition. So far, despite repeated efforts to raise these concerns, neither the government nor the PSR have provided any evidence that this will not happen.

EMA proposed way forward on APP scam reimbursement

170. The EMA considers that prior to implementing any measures for mandatory reimbursement of APP scams, the government must (1) carry out a consultation on the underlying assumptions behind mandatory compensation, and (2) conduct a proper impact assessment on the effects of mandatory compensation.

171. The consultation should explore the desirability of requiring PSPs and specialist PSPs in particular, to underwrite wider community fraud where PSPs have met their duty of care, and the impact on incentives for PSPs and other stakeholders to reduce the incidence of such APP scams. The consultation should consider the merits of penalising PSPs that have

met their standard of care, the distinctions and relative contributions of direct and indirect participants, and the disproportionate impact that FPS rules may have on new specialist and innovative PSPs.

172. In addition, we consider that a full assessment of the legal barriers to creating a balanced and proportionate liability framework for FPS should be conducted before moving directly to mandatory reimbursement via FPS scheme rules.

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

173. The EMA is reluctant to see the certainty of payment execution times set out in PSRs being eradicated without (a) strong evidence that this is a proportionate and appropriate response to address the specific types of fraud the proposed measures are intended to and can address; and (b) appropriate balancing against the interests of the payer and payee in any transaction, as well as that of any third party payment service provider, such as a PISP; and (c) appropriate safeguards to ensure it will not disproportionately and adversely affect legitimate payments. We elaborate on our concerns and considerations below.

The detrimental effect of delaying payments

(1) Efficiency of and trust in payment systems depend on immediacy and certainty of payments

174. The D+1 timeframe for the execution of payment orders as set out in Regulations 86 and 89 of PSR reflects an EU-wide PSD2 standard aimed at improving the efficiency of payments, and providing certainty to consumers on the length of time a payment can take. The certainty in payment execution timeframes is important for enabling financial and cashflow planning by consumers and businesses alike and reducing the time the funds are locked in transit in the financial system, which is ever more pertinent in the current economic climate (the cost of living crisis). Maintaining the D+1 standard is important in order not to undermine the trust of both the payers and payees (e.g. merchants) in the certainty provided by payment systems, the service provided by their payment service providers and competitiveness of the UK economy. A move toward less certain and slower payments would be damaging to innovation and competition in the payments sector, hindering the ability to offer new and/or improved products.

175. We note that in practice, payments are often expected to be completed in real time, which is the objective of Faster Payments scheme, so that D+1 is in fact a worst case scenario in these circumstances, and would be regarded as a failure to meet service levels, disrupting many commercial transactions. The impact of ability to delay payments needs to be balanced against the benefits of Faster Payments.

(2) The impact on payment recipients and their PSPs

176. We consider that a blanket approach allowing the sending PSP to delay payments that are suspected to be a result of fraud runs a high risk of disrupting legitimate transactions and is therefore inappropriate. Instead, careful consideration is required to ensure that the unintended consequences and the potentially damaging impact on the development of new payment methods, are avoided.

177. Accordingly, we consider it is important to ensure that the sending PSP's ability to delay payments is balanced against the interests of the payer and payee in any transaction, as well as that of any third party payment service provider, such PISP. The introduction of delays can be particularly harmful to the uptake and evolution of PIS services and their ability to compete with payment methods such as card payments. This would particularly be true if, in the event of the delay, the PISP who often has relationships with the payees, cannot assure the certainty of payment to its own customers or be informed of the reasons for the delay, undermining confidence in their own payment services when compared to alternative payment methods.

178. There must also not be an outcome where the current proposals provide the vehicle for de-risking certain sectors (e.g. deemed by the sending PSP as *potentially* higher risk), or certain types of PSPs. Such outcomes would be extremely damaging to innovation and competition in the UK market.

Slowing down of payments should only be permitted in narrowly defined circumstances

179. Considering the importance of immediate payments to commercial transactions, to efficient payment systems, and to user expectations, any exceptions to the D+1 service level legal obligations should be narrowly defined and very limited in scope.

180. It appears that the ability to delay payments in this way are *intended to,* but not limited to investigating suspected APP scams - it may be helpful to provide further clarity which types of fraud the delays in payments are permitted. Further, even if it were limited to APP fraud, the existing APP fraud/scam definitions are too broad (which may encompass, e.g. purchase scams, romance scams, investment scams, impersonation scams etc) - where the PSP's ability to detect or prevent any particular type of scam varies. In our view, it would be more proportionate to target specific types of APP scams with suitable anti-fraud solutions. This could mean, for example, that sending PSP should only be able to delay the execution of payments beyond D+1 on suspicion of a particular type of APP scam, where the PSP ability to prevent such scam and the value of the payment justifies it.

The ability to delay payments must not affect SEPA payments

181. It is of utmost importance to ensure that UK PSPs continue to be able to participate in SEPA to send and receive payments in euros. The EMA would not support any changes that could undermine such continued participation. It is understood that this means that SEPA payments should be left out of scope of the ability to delay payments and any

proposals to delay payments beyond D+1 for EURO transactions must be subject to agreement with the Eurosystem, and with the European Payments Council to avoid any impact on the UK's ability to continue to participate in the SEPA framework.

Limiting the impact on legitimate payments

182. Current business and user expectations are for payments to take place in real time, and D+1 timeframe (as required in regulation 86 PSR) provides a backstop with which PSPs comply where payments are not immediate in nature.

183. Commercial transactions require certainty of payment to be available immediately, and retail payments, particularly so. Any exception to this would therefore have an impact on both the specific transaction itself, whether it will be abandoned in favour of an alternative means of payment, or it will give rise to a complaint, but also on perception of the payment channel itself by retail users. Uncertainty will result in a preference for other means of payment that do not result in the same uncertainty.

184. In order to manage this risk, it is necessary to limit the scope of incidents where any delay beyond 'immediate payment' is likely to arise, and certainly any delay beyond D+1.

185. APP scams relate to a very broad genre of fraud, with varying visibility to the payer PSP on the one hand, to the payer themselves and to the payee's PSP. Creating a general allowance for investigations to be carried out in order to mitigate the risk of loss to the PSP is in our view detrimental to the payment product itself, reducing fraud by reducing its overall utility for any payments.

186. Any allowances to disrupt the payment flow and to do so beyond the D+1 limit must be subject to a number of conditions that limit the impact of the disruption. These could include the following conditions:

- The APP scam must be one that is capable of being observed by the PSP through monitoring, or of coming to their attention through other means such as suspicious destination accounts etc. A general allowance for all APP scams would bring in many categories of APP fraud, many of which are largely invisible to the PSP could require extensive investigation to determine their occurrence. In other words, the more remote a fraud is from the PSP, the more time will be required to uncover its circumstances and the more delay that will ensue.

- This is consistent with a more general condition that the scope of APP scams that PSPs would be expected to underwrite must also be those scams that are capable of being observed by the PSP. PSPs could be required to have appropriate monitoring and deterrence systems and practices, but cannot be expected to be held accountable for fraud that takes place in society as a whole and which they have little or no means of observing, detecting or preventing – even if the culmination of a successful fraud is an authorised push payment.

- Additionally, the value of the transaction must be such as to outweigh the impact of the disruption that will be caused by delaying the payment beyond D+1. There can be exceptions to avoid gaming of the thresholds by fraudsters, and these can be made subject to review by industry and regulators from time to time.
- There should be an absolute time limit following which the sending PSP could no longer delay the execution of a payment and would therefore have to execute the payment or refuse the payment. The absolute time limit can be set out in legislation. Such a time limit should take into account that the customer would not have access to their own funds during this time. Any such limit should be based on reasonableness.

187. We consider any circumstances enabling the delay beyond D+1 must go beyond "reasonable suspicion of fraud" or a similar standard, and must lay down conditions that must be satisfied, in order to safeguard the effectiveness of the payment system. This is particularly relevant when considering the role that Faster Payments plays in Open Banking solutions, and the dependence of this industry on certainty of payment.

188. Considering customer engagement, customers should be informed without delay by the sending PSP if their payment is delayed beyond reasonable user expectation, and certainly beyond D+1. However, any communication requirement should not put the sending PSP at risk of assisting the fraudster. In that respect, Regulation 82 of PSR provides a good precedent.

189. Finally, it must be recognised that the funds subject to any delay are those of payment service users, and users must have the right to dispose of their funds by whatever means they wish. Once warnings are adequately given, PSP should be able to release funds to users, but simultaneously cannot be held responsible for any fraud that follows.

21. In relation to fraud, whether unauthorised or authorised, is there a need to a) complement rules with data sharing requirements; and b) for further reforms be made to make Strong Customer Authentication work more effectively and proportionately?

Data sharing requirements

190. 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.

191. Data sharing arrangements should be encouraged, but not mandated. Industry-led data sharing projects are under discussion, and if adopted by a majority of PSPs, could have a substantial impact on fraud, while being flexible enough not to stifle innovation. The government's efforts and role should be focused on *enabling* data sharing. Policy support in this area may demand, for example, ensuring that data protection legislation enables such data sharing initiatives to take place without risk of non-compliance with data protection obligations.

192. For PSPs to participate in data sharing solutions, such solutions need to be accessible to all actors in the payment chain, and offered by multiple vendors. The solutions must also be available for access at a reasonable cost, in order to avoid effectively excluding smaller PSPs, to whom fraudsters may then migrate, as it would be more difficult for them to prevent fraud.

193. Data sharing must offer demonstrable benefits that outweigh the costs associated with data sharing; for certain types of fraud, increased payments data sharing will not improve the ability of PSPs to detect and prevent over and above their existing transaction monitoring controls. We consider that imposing a *requirement* for data sharing would therefore be inappropriate and disproportionate. It would have a big financial impact on firms, whilst hindering their ability to take measures aligned with their own approach to fraud and risk appetite, which vary vastly across different use cases and business models. The financial impact on firms, particularly smaller PSPs, while the industry is already implementing Confirmation of Payee, could be prohibitive, driving them out of the UK market. Additionally, the costs of implementing data sharing may be passed on to the consumer. Accordingly, the EMA considers that any proposals for mandated data sharing would have to be well researched and substantiated by an in-depth analysis of the costs and benefits of such proposals.

Strong Customer Authentication ("SCA")

194. We welcome the government's consideration, as part of this Call for Evidence, of introducing a more outcomes-based approach to authenticating payments. The EMA supports a review of the SCA requirements that focuses on defining the required security objectives, and affords PSPs flexibility on how to attain these objectives in high-risk payment account interactions. We believe that this is the right approach to enable firms to have the flexibility to innovate to meet evolving fraud threats, and to better meet the complex and diverse needs of their customers.

(1) The impact of current SCA requirements

195. The PSD2 approach has been to set out authentication requirements in legislation (PSR in the UK) and the associated Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Methods of Communication ("**SCA RTS**" - now retained as the FCA's Technical Standards, made pursuant to its standard-setting powers under regulation 106A of the PSR). The legislative requirements were further supplemented by clarifications in European Banking Authority Opinions[13] and in EBA responses to industry questions published in the Q&A section of the EBA website (largely reflected in the FCA's guidance in its Approach Document[14]). The volume of the regulatory clarifications that have been published and the scope of delays in implementing

[13] EBA Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04), EBA Opinion on the elements of SCA under PSD2 (EBA-Op-2019-06).

[14] https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf

the SCA requirements across different payment types (e.g card-based e-commerce transactions) speaks to the inefficiency of prescribing technical solutions in a legislative text.

196. The impact of prescribing authentication solutions in legislative text and providing implementation guidance in SCA RTS has been as follows:

- It is generally accepted that the initiation of payment transactions where SCA is applied involves more friction on the PSU. Current SCA rules emphasise the use of active authentication techniques, with explicit customer intervention; this approach limits choice and degrades the customer experience, when frictionless (passive authentication) solutions might also be available.
- There are elements of SCA that are disproportionately resource-intensive, costly or that have eroded user convenience through friction.
- The SCA rules limit the number of options/technologies available to PSPs. For instance, most SCA strategies combine passwords (knowledge) with some form of device-based authentication factor as possession evidenced through the use of a real-time token.
- The current treatment of all payment account interactions (as set out in regulation 100 PSR) as a trigger for SCA ignores the different risk profiles of in-scope interactions (*balance/history look up, payment transaction initiation/execution, account profile lookup/revision*). This monolithic treatment has resulted in multiple SCAs being performed by payment ecosystem participants to complete a single payment transaction, introducing unnecessary friction and poor customer experience. Examples include (i) the use of digital wallets to initiate a payment when both the wallet funding and the outward payment transaction require SCA; or (ii) combined AIS/PIS payment account accesses where a user first reviews account information before initiating a payment transaction. The current approach also inhibits the use of user authentication frameworks that leverage "adaptive authentication" to reflect the varying risks of account interactions, which can preserve current SCA PSU security benefits while minimising friction.
- The requirement to apply SCA (and Dynamic Linking) has severely impacted the use of remote payments in certain use cases (e.g. travel, entertainment) that involve the use of service delivery intermediaries and aggregators. Continued operation of payment solutions for these use cases in many cases demands reliance on sector-specific SCA exemptions/waivers from the regulator, i.e. the FCA.
- SCA requirements are overly prescriptive and reflect legacy technologies. Detailed SCA and SCA exemption requirements prescribed in the SCA RTS have imposed costs on PSPs significantly beyond those originally envisaged. PSPs have expended time, effort and costs in understanding, preparing for and implementing solutions compliant with regulatory technical standards that have a short shelf life, hindering innovation and competitiveness in the market.

- There is industry evidence[15] pointing to increased numbers of dropped/abandoned remote electronic payment transactions after the requirement for full SCA compliance started to apply to credit transfers (14th September 2019) and to payment cards (March 2021). There is also anecdotal evidence of similar rates of user abandonment at the point of interaction in the application of SCA in other channels. The estimated costs associated with the SCA rollout in the EU have been significant, notably implementation costs (estimated at ~ EUR 5 billion) and an increase in transaction failure rates (estimated at up to EUR 33.5billion).[16]

197. We note also that the adoption of a prescriptive approach to implementing SCA in legislation - rather than setting out a set of security objectives to be attained through the use of SCA implementation approaches - may give rise to greater systemic payment ecosystem security risks. Attacks that target a specific SCA implementation can impact the entire payment ecosystem. The adoption of a prescriptive SCA implementation approach in legislation that changes slowly can also limit innovation and the use of novel technologies that are showing potential to address payment security risks (AI, machine learning).

198. In short, the payments security principle is welcome, but the means of implementation of SCA requirements requires revision.

(2) SCA and fraud

199. As we elaborate further below, the SCA has reduced fraud but at the cost of significantly reducing successful completion of transactions. The 2022 Annual UK Finance Fraud Report[17]18 records a 9% drop in the value of online (Card not Present – "**CNP**") transactions in the UK. These figures record the impact of the application of SCA on card-based CNP transactions post the end of March 2022.The EMA members have also witnessed a migration towards manipulation of the payer (authorised push payment) fraud, which SCA does not address.

200. EMA members report a reduction in fraud rates since the introduction of SCA, but there has also been a sharp drop in successful transaction completion rates and widespread use of SCA exemptions in order to counteract the negative impact on user experience.

201. EMA members also point out the ongoing payment fraud migration to typologies that cannot be counteracted through the use of SCA (e.g. social engineering attacks leading to

---

[15] Card Scheme (MCI) data from Q1/Q2' 2021 indicates c.22% of all browser-initiated card transactions and to 53% of in-app card transactions failed to complete Issuer Step Up (Soft Declines).

[16] European Commission, 'A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)', available at https://op.europa.eu/en/publication-detail/-/publication/f6f80336-a3aa-11ed-b508-01aa75ed71a1/language-en

[17] https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2022

authorised push payment fraud) and an increase in average fraud incident value as fraudsters attempt to maximise their "return on investment".

(3) SCA exemptions

202. Payment industry participants have attempted to manage the impact of this blanket regulatory treatment of different payment account interactions for SCA purposes by making use of SCA exemption or exclusions. For example, Merchant Initiated Transactions – "**MITs**" - which are outside the scope of SCA requirements. However, there is growing industry concern that this may not be a viable, long-term approach. If MITs were to be moved within the perimeter of SCA requirements, the payment industry would suffer significant additional disruption.

203. Mail order/telephone order ("**MOTO**") transactions are also currently out of scope of the SCA requirements unless a remote electronic channel is used to initiate such transactions. Our view is that MOTO transactions should remain out of scope SCA requirements since they experience low levels of fraud.

204. Separately, we consider that refunds, even if technically initiated by the payer (merchant) should not be subject to the SCA requirements. Due to their nature, such payment transactions experience low levels of fraud; applying SCA to such payments introduces an unwarranted level of friction/delays for processing refunds, potentially resulting in poor merchant customer experience. As such, we would welcome a clarification on scope of the SCA requirements as being not applicable to refund transactions.

205. Finally, the requirement to apply SCA (and Dynamic Linking) has severely impacted the use of remote payments in certain use cases (e.g. travel, entertainment) that involve the use of service delivery intermediaries and aggregators. Some of these use cases continue to operate on the back of sector-specific SCA exemptions granted by the FCA.

206. To the extent that the SCA requirements are reformed, we would urge the government and the FCA to ensure that transaction types and payment account interactions currently excluded from SCA requirements remain out of scope. Increasing the scope of payment transaction types that trigger SCA will further disrupt PSP operations and add further friction to customer experience. Any increase in the scope of payment transaction types that trigger SCA will further disrupt PSP operations and add further friction to customer experience.

(4) Future approach to SCA

207. We have described above the impact of setting out an authentication solution in legislative text, as opposed to defining strong customer authentication and required security objectives. The latter approach would allow industry to innovate and keep up with evolving threat vectors; the identification of specific technological solutions in legislative text hinders development and innovation. We would therefore support the revision of the SCA requirements to enable the application of SCA in a risk-sensitive manner and to focus on payment account security objectives rather than specifying acceptable authentication element types.

208. Avoiding a prescriptive approach and setting out a set of security objectives can help minimise systemic payment ecosystem security risks. A legislative approach that allows the use of alternative authentication mechanisms that can demonstrate equivalent strength to the current definition of SCA (e.g. one or multiple authentication elements of the same type coupled with additional PSP layered data) to attain the stated security objectives can increase SCA implementation options for PSPs, decrease operational costs, deliver an improved PSU experience and diminish systemic risks associated with the use of a single SCA implementation strategy.

209. Furthermore, SCA requirements should be revised to adopt a risk-based SCA application approach whereby SCA is only applied where necessary (i.e. for high-risk payment account interactions). Such an approach would reduce the likelihood of legitimate transactions being declined and lower transaction abandonment rates. Allowing PSPs to deploy holistic user authentication frameworks that leverage "adaptive authentication" approaches to reflect the varying risks of attempted payment account interactions can preserve current SCA PSU security benefits while minimising friction in the customer experience.

210. We therefore suggest a revision of regulation 100(1) PSR to:

- Afford greater PSP flexibility to apply SCA only in higher risk payment account interactions. PSPs could still be required to apply appropriate customer authentication techniques (e.g. leveraging a single authentication element type) for lower-risk interactions.
- Define more narrowly the payer's activities that must trigger SCA. Specifically, condition (c) should be revised to identify the actions - carried out over a remote channel - that must trigger SCA.

211. The specification of SCA exemptions should continue to be included in the FCA's Technical Standards or regulatory guidance that can be revised more frequently to address evolving fraud threats.

212. Finally, whilst a revision of the SCA requirements is much needed and welcome, we are conscious of the impact that the divergence from PSD2/PSD3 requirements in that regard may have. In particular, increasing divergence may increase the operational costs for PSPs and/or minimise the benefits to be had from any resulting SCA requirement changes. We ask the government to continue taking into account the impact of divergence from the EU rules in that regard.

SCA for AIS

213. The application of SCA for AIS, and in particular the requirements for re-authentication, presented significant challenges to the AIS providers when the PSRs were first introduced. We welcomed the FCA's intervention and amendments to the UK RTS on SCA in 2021 to address these issues and support the nascent AIS ecosystem.

214. However, the application of the exemption in Art 10A of the RTS on SCA remains voluntary and this has led to an inconsistent experience for users of AIS services, which in turn continues to suppress innovation and competition.

215. In line with a risk-based approach to applying SCA, we believe that there is scope to further address the application of SCA to AIS. We suggest that HMT consider options such as (i) making Art 10A exemption mandatory for all ASPSPs, or

(ii) enabling AISPs to apply SCA, instead of the ASPSP (once the initial data access connection has been established with an SCA with the ASPSP).

Issuance and redeemability of electronic money[19]

Considered against the government's objectives for payments regulation:

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

216. The EMA considers that the e-money issuance and redemption requirements are still appropriate. In fact, these requirements pertain to the legal rights of the e-money holder against the issuer, and underpin the legal attributes of e-money; it is therefore important that they are retained.

Miscellaneous

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

No comment.

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

217. We have a number of comments regarding the framework for the rights and obligations between the PSPs and their PSUs as set out under Part 7 PSR, which are as follows:

- **Low-value payment instruments (regulation 65 PSR):** reduced obligation requirements under regulation 65 PSR apply to certain low value payment instruments - the values set out under this regulation should be increased. We make the same comments as those set out in response to Q10 in relation to the information requirements under PSR Part 6. The values under regulation 65 should be increased to reflect inflation and utility of instruments. We consider an increase in value to EUR 100 for individual transactions (regulation 65(1)(a)), spending limits to EUR 500

[19] Part 5 of the Electronic Money Regulations

(regulation 65(1)(b)), and storage limits to EUR 1,000 (regulation 65(1)(c)) to be reasonable.

- **Micro-enterprises (regulation 63(5) PSR):** We repeat our comments set out in response to Q10 as regards the problems associated with the requirement to treat micro-enterprise customers as consumers. For the same reasons, we suggest that regulation 63(5) would benefit from revision to remove the mention of micro-enterprises. The revised regime could continue to include individual business customers, such as sole traders, to benefit from the same treatment as consumers.

  Further, we believe there is merit in extending the corporate opt-out provisions at regulation 63 PSR to a broader range of requirements under Part 7 of PSR. In the alternative, for those Part 7 requirements the government considers should apply to business customers and payment services as a standard, a specific exemption for corporate payment services could be introduced - Article 17 of the SCA RTS exemption for secure corporate payments provides a precedent in that regard.

  We believe that such changes would provide much needed flexibility, in line with the objectives for proportionate and agile regulation, given the different nature of corporate payment services market, whilst at the same time ensuring that business payments continue to benefit from core regulatory standards set out in the PSR. PSPs that service corporate PSUs should be able to better tailor their services, including the security and risk management processes, to the needs of corporate PSUs. At the same time, corporate PSUs are in a better position than consumers to negotiate bespoke arrangements and appropriate contractual protections, they are unlikely to be prejudiced by having the ability to opt out of a broader range of provisions under the PSRs.

- **Payer's liability for unauthorised transactions (regulation 77(1)):** the maximum liability for a payer as set out in this regulation should be increased. We consider an increase to GBP 100 to be reasonable. This would reflect inflation as well as discourage carelessness or reckless behaviour of payers, in looking after their payment instruments or the security credentials used to access them.

Members of the EMA, as of April 2023

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
Amazon
American Express
ArcaPay UAB
Banked
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
CashFlows
Checkout Ltd
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
FIS
Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
J. P. Morgan Mobility Payments Solutions S. A.
Modulr Finance Limited
MONAVATE
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Payments Ltd
Nuvei Financial Services Ltd
OFX
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Park Card Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Paysend EU DAC
Plaid
PPRO Financial Ltd
PPS
Ramp Swaps Ltd
Remitly
Revolut
Ripple
Sable International FX Limited
Securiclick Limited
Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Swile Payment
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
ValletaPay
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wirex Limited
Wise

WorldFirst
Yapily Ltd