Electronic Money Association
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

To
Amendments to the Money Laundering Regulations 2017 Consultation
Sanctions and Illicit Finance Team
HM Treasury
1 Horse Guards Road
SW1A 2HQ

Anti-MoneyLaunderingBranch@hmtreasury.gov.uk

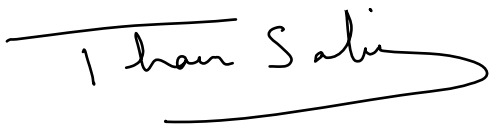
Dear Shantel

Re: Amendments to the Money Laundering Regulations 2017 Statutory Instrument 2022 Consultation

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

We welcome the opportunity to comment on the draft changes to the MLRs 2017 Statutory Instrument 2022. We have not responded to every question in the consultation. I would be grateful for your consideration of our comments and proposals.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response

1. **What, in your view, are the ML/TF risks presented by AISPs and PISPs? How do these risks compare to other payment services?**

The EMA agrees with HMT's assessment in the consultation document that the inherent ML/TF risk presented by AISPs and PISPs is low and for PISPs in particular, consider that their role as intermediaries between payment service users and other financial institutions, may reduce the risk of money laundering within the payment chain.

Taking each service in turn:

Payment Initiation Services (PIS):

PIS products enable the initiation of transactions from one regulated payment account holding (servicing) payment service provider to another; both of which will be regulated for prudential, conduct, financial crime risks, and will have put in place CDD, monitoring and reporting processes and controls. The PISP is responsible for generating payment orders based on a request from the payment service user (PSU) and does not influence the execution of the payment. The payment order simply represents the PSU's instruction to initiate the payment and, just as when banks receive payment orders from customers, it is the bank's responsibility to decide whether to execute the transaction or not.

PIS providers do not open payment accounts and cannot hold user funds, nor can the PISP influence the size, frequency or timing of transactions, other than refusing to initiate a transaction entirely. The ML/TF risk is therefore not increased by the use of a PISP as compared to the customer submitting the payment order themselves directly to the bank. In some cases, the presence of the PISP in the payment chain may act to reduce ML risk, as the PSU is required to expose their activities to an additional financial institution.

Account Information Services (AIS):

AIS products involve no initiation or execution of payment transactions; AISPs have read-only access to customer bank account information and the AISP cannot conduct any financial transactions on a payment account. AISPs cannot influence any kind of activity that could give rise to money laundering and are simply independent observers of the activities undertaken by their customers.

It is arguable that without specific consent and authority, AIS providers are not entitled to review their customers' data, which originated elsewhere and to do so would be an abuse of their customers' expectations of trust and confidentiality. Given that all financial services related data will have already been reviewed, and be subject to monitoring and reporting obligations by the relevant account service provider, this emphasises the duplication of effort and further reinforces the absence of a nexus between an AIS service and anti-money laundering risk mitigation objectives.

2. In your view, what is the impact of the obligations on relevant businesses, in both sectors, in direct compliance costs?

AISPs

Historically, a significant proportion of AIS services are provided at no cost, or no additional cost, to SMEs and consumers. Firms new to the market, as well as existing providers, have required significant investment in order to comply with ML/TF requirements to which they have no exposure as they do not move funds. For some AISPs, this compliance cost puts their long-term product proposition and business model at risk.

For example, the appointment of an MLRO in itself is a prohibitive cost for an AISP - with salaries for London based fintech MLROs at around £80K - £100K (according to Glassdoor). In addition, our Members estimate the cost of interpreting AML rules, obtaining legal advice, building monitoring systems and processes to be in the hundreds of thousands of pounds. This is a large burden for AISPs establishing themselves in the market

Customer Due Diligence

ASPSPs are obliged to conduct customer due diligence when a payment account is opened and personalized security credentials are issued to the account holder to access that account online, Further, AISPs rely on these security credentials for authentication of the PSU for any access to a payment account[1]. This means the identity of the account holder is being established, with the same degree of certainty that applies to the ASPSP, every time an AISP accesses payment account data.

JMLSG guidance notes "..*several firms requesting the same information from the same customer in respect of the same transaction not only does not help in the fight against financial crime, but also adds to the inconvenience of the customer*."[2]

Hence any additional identity and verification measures conducted by the AISP is wholly redundant as it will not produce any further transparency in order to reduce ML risk.

Transaction Monitoring

AISPs are required to gain their customer's explicit consent to read their payment account data, and must clearly inform the customer of the purpose and use of that shared data. In addition, the Payment Service Regulations (PSRs) require that AISPs "*must not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules*."[3] These obligations in effect mean that the AISP has to gain the PSU's consent to monitor their payment account activity for any purpose that possibly directly conflicts with the PSU's expectations of the AISP's service.

[1] Art 100 (1) and (4), Payment Services Regulations 2017

[2] JMLSG Part 1, paragraph 5.6.2

[3] Art 70 (3)(f), Payment Services Regulations 2017

Furthermore, as the consultation document states, the purpose of the MLRs are "*to detect and prevent money laundering and terrorist financing before it occurs*"[4] . However, most AISPs only access a rolling snap-shot of transaction data on a payment account, which may in fact be an extremely narrow view of the account data depending on the PSU's instructions to the AISP. This limited data-set runs counter to the objective of the MLRs and significantly reduces the AISP's ability to conduct robust on-going transaction monitoring. The AISP can potentially only identify suspicious activity after the event, has no means of assessing the purpose of transactions, and will not have any sight of accounts held by its customers with institutions to which it has not been granted access. Besides, the AISP has no ability to stop transactions, and is only ever in a position to observe possible historical suspicious activity, which does not strengthen the ASPSP's ML controls.

In all cases, the ASPSPs are subject to the MLRs and are required to conduct the necessary payment account holder due diligence and monitoring of transactions for suspicious activity. Hence requiring AISPs to duplicate AML control measures is redundant, serves no purpose in mitigating against money laundering risk, and places unnecessary compliance overhead on firms.

PISPs

In the payment flow, the PISP can interact directly with both payment service user (PSU - payer) and the payee. The PISP can have a business relationship with either one of them or both. However, for most current PIS business models, the PISP's customer is the payee (merchant). Although transactions are initiated with the payer's PSP, the PIS payment service that is facilitated from the payer, is delivered to the payee. In this regard the service provided by the PISP is similar to that of a card acquirer (or processor) in the payment flow, but the PISP does not come into possession of funds during the transaction.

Customer Due Diligence

The EMA considers that PISPs offering services to merchants have faced a misinterpretation of the MLRs where it is erroneously considered that the payer (whose account the transaction is initiated from) is also always their customer, and that ML/TF requirements should therefore apply. For the most part however, the occasional transaction approach will apply in this scenario, as the PISP will not have an on-going business relationship with the payer.

Where PIS services are provided to the merchant (payee), such as in an e-commerce scenario, conducting CDD on the payer introduces significant friction to the customer journey because, as a minimum, the PISP would have to interrupt the checkout process so that the PSU's identity information is captured during the check-out process. This places PIS payments at a disadvantage in comparison to other payment instruments (such as cards) in terms of ease of use, and also raises competition issues with other PSPs who provide similar services to merchants (such as card acquirers), who are not obliged to conduct CDD on the payer.

[4] Paragraph 1.3 - Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022 Consultation

Carrying out CDD at the point of sale not only leads to PSUs abandoning the PIS service, but also makes the cost of providing PIS prohibitive; costs which would have to be passed on to the merchant and have the potential to prevent the adoption of innovative PIS propositions.

It is possible for the PIS service to be delivered directly to the payer in different circumstances. For example:

- an App facilitating payments from accounts belonging to the payer, on the instruction of the payer;
- perhaps in a semi- automated manner, choosing the most appropriate payment instrument for different payment transactions, or
- making periodic push payments on behalf of the payer when other criteria are fulfilled.

In these cases, the payment service is certainly delivered to the payer, and the PISP does not have a relationship with the payee.

Equally, our arguments regarding duplication of cost and effort on the part of AISPs conducting CDD of the payer apply to PISPs. The ASPSP is obliged to conduct customer due diligence when a payment account is opened and when issuing the personalized security credentials to access that account online. PISPs rely on these security credentials for authentication of the PSU for every payment initiation[5]. This means the identity of the account holder is being established with the same degree of certainty that applies to the ASPSP, every time a PISP initiates a transaction. Any additional identity and verification measures conducted by the PISP are unnecessary and do not mitigate any further against ML risk.

Transaction Monitoring

Furthermore, PISPs are prohibited by Article 69, 3(g) PSRs from "*use, access or store any data*", other than for the purpose of providing the payment initiation requested by the PSU. Yet the ML/TF obligations require obligated entities to scrutinise the transactions undertaken by a customer to identify unusual transactions, patterns of transactions or behaviour. Given their PSR obligations, it is not clear how a PISP will be able to seek information on the purpose of transactions or store sufficient transaction data to fulfil this ML obligation.

Given the PISP is not involved in the execution of the transaction and the immediate nature of credit transfers, the only measure a PISP can take to prevent a suspicious transaction is to refuse to initiate it.

Lack of complete information to assess a transaction may also give rise to defensive reporting by PISPs, as well as multiple SAR reporting, given that the relevant ASPSP will have also have submitted a SAR on the same transaction where required.

3. **In your view, what is the impact of such obligations dissuading customers from using these services? Please provide evidence where possible**.

PSD2 (and the Payment Services Regulations in the UK) was introduced to increase innovation and competition – providing consumers and businesses with more choice and options. The

[5] Art 100 (1) and (4), Payment Services Regulations 2017

application of AML requirements to AISPs and PISPs is counterproductive to the purpose of this regime.

The onboarding experience is typically responsible for shaping a customers' ongoing expectations about the quality of service that they can expect from a provider. This is particularly the case when considering nascent services such as AIS and PIS, which are often new to the customer.

Account servicing providers (ASPSP) are required to take steps to identify and verify the identity of their customers at account opening and on an on-going basis. Art. 100 of the PSRs requires Strong Customer Authentication (SCA) to be applied when accessing a payment account or initiating a payment, including when account data is being accessed using an AISP, or a transaction initiated by a PISP. Accordingly, the identity of the PSU is being established and confirmed by the ASPSP for every AIS or PIS interaction under the PSRs in a secure and reliable manner, additional identity checks carried out by AISPs or PISPs are unnecessary and add wholly disproportionate friction to the customer's use of their services.

Requiring AISPs and PISPs to perform customer due diligence also creates an unlevel playing field with incumbent payment service providers (such as banks and card providers) who decide to offer AIS or PIS, as they will have already applied customer due diligence measures when a payment account is opened, and are unlikely to repeat CDD when offering AIS or PIS to existing customers.

Specific Impact of AML obligations on take-up of PIS

As discussed in our response to Q2, AML obligations risk making open banking payments (specifically PIS payments to businesses) unworkable as a competitor to cards and other payment methods. This would prevent one of the key objectives of the Payment Services Regulations (PSR), which was to introduce competition in retail payments.

In a normal card purchase scenario, a customer goes to the check-out, enters their card details and delivery information with the merchant, and approves the transaction (including passing security with the bank where necessary using strong customer authentication). The purchase is complete. The customer (PSU) does not have to provide KYC or customer due diligence information to its payment service provider (e.g. the card issuer) at the point of sale. This is because the customer has already provided this information to the card issuer when they opened a card or bank account. The card acquirer does not have to obtain CDD from the customer, because the acquirer's business relationship is with the merchant (providing a payment service to the merchant - its customer).

In a similar manner PISPs who are offering a PIS payment method on a merchant's website provide the payment service to the merchant, and may not have a relationship with the payer at all. To interrupt the payment flow at the check-out, in order to undertake KYC/ CDD would undoubtedly lead to customers abandoning purchases and not using open banking (PIS) as a payment method again.

In order to ensure that PISPs can provide a seamless experience at the checkout for retail payments (equivalent to cards), it needs to be clarified in the ML Regulations and guidance that

the PISP's customer for the purpose of ML obligations, can be determined to be the business being paid (the payee), rather than the payer/ payment service user

4. In your view should AISPs or PISPs be exempt from the regulated sector? Please explain your reasons and provide evidence where possible.

The EMA believes that both AISPs and PISPs should be exempted from the UK's money laundering regime. ML/TF obligations for AISPs and PISPs do not serve the purpose for which they were intended, are disproportionate to the risk of money laundering or terrorist financing occurring, as well as burdensome for firms, and redundant within the wider financial system. For these reasons, we do not consider exempting AISPs and PISPs will affect the objective of the UK's money laundering regime, nor expose the financial system to further ML/TF risks.

We acknowledge that HMT are considering maintaining PISPs within the regulated sector. Should PIS providers remain within the scope of obligated persons, given that such a service gives rise to a low risk of money laundering, the controls that are put in place should be calibrated accordingly.

We ask that HMT address a number of key areas where the ML obligations have affected PISPs ability to offer services, and ultimately on the customer take-up of innovative and competitive propositions. In summary:

- **Identifying the PISP's customer** - we would welcome further clarification in the MLRs and clear guidance on the relative roles played by a PIS provider in relation to payer and payee to avoid invoking unnecessary ML obligations, and adversely affecting innovation PIS propositions from being launched in the market.

  This issue has been acknowledged by the European Banking Authority in its Sector Guidelines on AML Risk factors. It clarified the definition of customer in Guideline 18.8 '*in order to confirm that PISPs should assess whether they have a business relationship in the meaning of Article 3(13) of the AMLD with the payer and/or with the payee, and other circumstances set out in Article 11 AMLD, in order to conclude who the customer is, and, more specifically, to emphasize that PISPs do not always enter into a business relationship in the meaning of Article 3(13) of the AMLD with the payer*'

  The EU's proposal for a new regulation on AML/CFT also addresses this issue::
  Recital 34: Some business models are based on the obliged entity having a business relationship with a merchant for offering payment initiation services through which the merchant gets paid for the provision of goods or services, and not with the merchant's customer, who authorises the payment initiation service to initiate a single or one-off transaction to the merchant. In such a business model, the obliged entity's customer for the purpose of AML/CFT rules is the merchant, and not the merchant's customer. Therefore, customer due diligence obligations should be applied by the obliged entity vis-a-vis the merchant.

In our view, this provides clearer direction to PISPs than the EBA's AML guidelines, and the definition of 'customer'.

We make the following suggestions for ensuring that PISPs can continue to provide payment services that are competitive with other payment type:

- The MLRs should provide PISPs with the ability to assess whether they have a business relationship in the meaning of the MLRs with the payer and/or with the payee
- It should be made clear that PISPs do not always enter into a business relationship in the meaning of the MLRs with the payer (the PSU), but that the business relationship can be with the payee.
- It should be made clear that when a business relationship is made with the payee (not the payer), the customer for the purposes of the MLRs, is the payee, not the PSU

- **Access to identification information** – were the PISP to apply CDD measures to the payer in the merchant customer model, then, given the linear nature of the transaction, it would make most sense for identification information to be made available by the payer's ASPSP through the API that is accessed by the PISP. This is not unlike transactions in other parts of the financial services sector, where brokers and other parties are involved in a single sale or payment. The different parties will share the identification, and frequently the verification information that is performed by one of the parties, usually the broker.
- **Sharing of monitoring-related data by ASPSPs and PISPs** could enhance both parties' ability to monitor and identify unusual and suspicious activity. It would be helpful if the ASPSP and the PISP were to exchange data that would render the information that they hold more meaningful and enable a more effective monitoring and unusual transaction detection capability. This could comprise enhanced data on the identity of the customer, their location, IP address or other relevant data that could be called by either party through the API.

BPSPs and TDITPSPs

5. In your view should BPSPs and TDITPSPs be taken out of scope of the MLRs? Please explain your reasons and provide evidence where possible.

The current MLRs provide for the inclusion of unregulated bill PSPs for example acting as commercial agents, as well as IT network service providers such as mobile network operators extending unregulated payment services to their customers. HMT has stated that these are regarded as low risk, and provided this is the case, and continues to be the case, the EMA is supportive of a proportionate approach to the application of AML Regulation. The EMA therefore does not object to the removal of these service providers from the scope of AML regulation.

6. **In your view, if BPSPs and TDITPSPs were to be taken out of scope of the MLRs, what would the impact be on registered businesses, for example any direct costs? Are there other potential impacts?**

7. **Would the removal of the obligation for PSPs to register with HMRC for AML supervision, in your view, reduce the cost and administrative burden on both HMRC and registered businesses?**

8. **In your view, would there be any wider impacts on industry by making these changes?**

SARs

13. **In your view, is access by AML/CTF supervisors to the content of the SARs of their supervised population necessary for the performance of their supervisory functions? If so, which functions and why?**

SARs should continue to be submitted exclusively to the NCA, who should continue to have the ultimate responsibility to share information with governmental authorities as necessary for the prevention or detection of money laundering or terrorist financing.

Using SARs as a tool for supervision would distract from their actual purpose. Firms should be able to report SARs to the FIU without having to consider whether the content would prompt the supervisor to investigate them or any other firm that is mentioned in a particular SAR. Scrutiny from the regulator may impact the content of SARs, and firms may not disclose details that they would have otherwise provided to the FIU.

Requiring the industry to inform their supervisor(s) of the content of SARs could give rise to a dual-reporting obligation, which is not efficient and would require significant operational effort. In addition, firms expect the burden of reporting would not end with the submission of a SAR, but would likely lead to follow-up questions and requests for further data or evidence.

14. **In your view, is Regulation 66 sufficient to allow supervisors to access the contents of SARs to the extent they find useful for the performance of their functions?**

15. **In your view, would allowing AML/CTF supervisors access to the content of SARs help support their supervisory functions? If so, which functions and why?**

It is unclear what purpose the sharing of SARs would serve in the context of supervision - SARs are a tool for law enforcement to fight financial crime, which is outside the remit of AML supervisors.

16. **Do you agree with the proposed approach of introducing an explicit legal requirement in the MLRs to allow supervisors to access and view the content of the SARs**

submitted by their supervised population where it supports the performance of their supervisory functions under the MLRs?

We do not agree. If AML supervisors wish to view SARs, they should request the content of SARs directly from the FIU.

17. In your view, what impacts would the proposed change present for both supervisors and their supervised populations, in terms of costs and wider impacts? Please provide evidence where possible.

Requiring the industry to inform their supervisor(s) of the content of SARs could give rise to a dual-reporting obligation, which is not efficient and would require significant operational effort. In addition, firms expect the burden of reporting would not end with the submission of a SAR, but would likely lead to follow-up questions and requests for further data or evidence.

As mentioned earlier scrutiny from the regulator may impact the content of SARs, and firms may not disclose details that they would have otherwise provided to the FIU.

18. Are there any concerns you have regarding AML/CTF supervisors accessing and viewing the content of their supervised populations SARs? If so, what mitigations can be put in place to address these? Please provide suggestions of potential mitigations if applicable.

Credit and financial institutions

19. In your view, what are the merits of updating the activities that make a relevant person a financial institution, as per Regulation 10 of the MLRs, to align with FSMA?

There is merit in substituting references to European legislation with those in domestic law. From our perspective, however, this is a merely formal change.

20. In your view, would aligning the drafting of Regulation 10 of the MLRs with FSMA provide clarity in ensuring businesses are aware of whether they should adhere to the requirements of the MLRs? Please provide your reasons.

We are not aware of an issue with clarity about the application of the MLRs to e-money institutions, payment institutions and cryptoasset service providers.

21. Are you aware of any particular activities that do not have clarity on their inclusion within scope of the regulated sector?

None that we are aware of.

22. **In your view, what would be the impact of implementing this amendment on firms and relevant persons, both in terms of direct costs and wider impacts? Please provide evidence where possible**.

None if no substantive changes in scope result from this change.

23. **In your view, what would be the impact of implementing this amendment on the FCA, both in terms of direct costs and wider impacts? Please provide evidence where possible.**

24. **In your view, would there be any unintended consequences of aligning Regulation 10 of the MLRs with FSMA, in terms of diverging from the EU position?**

Care would need to be taken to include the relevant activities regardless of whether they are carried out by credit institutions - an example would be the issuance of e-money, which can be undertaken both by credit and financial institutions.

25. **Do you agree with the proposal to use the FATF definition of proliferation financing as the basis for the definition in the MLRs?**

The EMA supports the proposal to use the FATF definition of proliferation financing as the basis for the definition in the MLRs, as it provides a harmonised definition at international level.

26. **In your view, what impacts would the requirement to consider PF risks have on relevant persons, both in terms of costs and wider impacts? Please provide evidence where possible.**

The EMA does not foresee any significant impact in terms of cost, as the requirements relating to PF risks are similar to other existing requirements relating to ML-TF.

27. **Do relevant persons already consider PF risks when conducting ML and TF risk assessments?**

PF risks are already taken into account through the application of sanctions.

28. **In your view, what impact would this requirement have on the CDD obligations of relevant persons? Would relevant persons consider CDD to be covered by the obligation to understand and take effective action to mitigate PF risks.**

29. **In your view, what would be the role of supervisory authorities in ensuring that relevant persons are assessing PF risks and taking effective mitigating action? Would new powers be required?**

30. **In your view, does the proposed drafting for this amendment in Annex D adequately cover the intention of this change as set out? Please explain your reasons.**

41. **Do you agree that the obligation to report discrepancies in beneficial ownership should be ongoing, so that there is a duty to report any discrepancy of which the**

relevant person becomes aware, or should reasonably have become aware of? Please provide views and reasons for your answer.

The burden of identifying and reporting discrepancies should not only be on obliged entities. It appears to be disproportionate to require ongoing reporting from PSPs, in comparison to the burden on other actors such as Companies House. Obliged entities cannot be expected to be the only actors collecting data, verifying it and reporting discrepancies.

Additionally, the term 'ongoing' is unclear, and does not indicate under what circumstances a firm should report. It should be explicitly stated that the obligation to report a discrepancy applies only when the discrepancy is discovered, i.e. for example when conducting a CDD refreshment cycle.

The EMA would also welcome a change to the legislation to allow firms to report discrepancies 'in bulk', possibly one a week or fortnight, in order to limit the financial impact that this new requirement will create.

42. **Do you consider there to be any unintended consequences of making this change? Please explain your reasons**.

The added administrative burden on firms would remove resources away from the areas of highest AML/TF risk. Instead Companies House should be responsible for verifying information and identifying discrepancies.

43. Do you have any other suggestions for how such discrepancies can otherwise be identified and resolved?

The issue is not only in the reporting of discrepancies, but mainly in the accuracy of the information provided to Companies House in the first place, and the lack of verification conducted by Companies House.

44. In your view, given this change would affect all relevant persons under the MLRs, what impact would this change have, both in terms of costs and benefits to businesses and wider impacts?

The benefits of the proposed measure remain unclear, as PSPs already have measures in place to mitigate UBO-related risks. However, as previously stated, the cost of such a measure - both for individual firms, as well as industry as a whole - would be high, as this new reporting would be very time consuming. This is exacerbated where the reports must be made one by one.

45. Would it be appropriate to add BEIS[6] to the list of relevant authorities for the purposes of Regulation 52?

We do not agree with the proposal to share information with Companies House ("CH") under Regulation 52. Obliged entities must report discrepancies under Regulation 30A; these reports should provide CH with sufficient information to improve the data held on companies and to support any investigations. Ideally, CH data should be verified to a level that would allow firms to rely on CH for customer due diligence purposes.

46. Are there any other authorities which would benefit from the information sharing gateway provided by Regulation 52? Please explain your reasons.

47. In your view, should the Regulation 52 gateway be expanded to allow for reciprocal protected sharing from other relevant authorities to supervisors, where it supports their functions under the MLRs?

Yes.

48. In your view, what (if any) impact would the expansion of Regulation 52 have on relevant persons, both in terms of costs and wider impacts? Please provide evidence where possible.

49. In your view, what (if any) impact would the expansion of Regulation 52 have on supervisors, both in terms of the costs and wider impacts of widening their supervisory powers? Please provide evidence where possible.

51. Is the sharing power under regulation 52A(6) currently used and for what purpose? Is it felt to be helpful or necessary for the purpose of fulfilling functions under the MLRs or otherwise and why?

52. What regulatory burden would the proposed changes present to Annex 1 financial institutions, above their existing obligations under the MLRs? Please provide evidence where possible.

53. In your view, is it proportionate for the FCA to have similar powers across all the firms it supervises under the MLRs? Please explain your reasons.

It is unclear whether e-money institutions and payment institutions are included in this proposed change, as these are financial institutions that are not authorised under FSMA. E-money institutions are subject to a separate prudential regime under the Electronic Money Regulations 2011 and payment institutions under the Payment Services Regulations 2017. Powers under FSMA "to oversee the prudential strength of Annex 1 institutions or their treatment of consumers" (para. 5.15 of the consultation document) should therefore not be introduced indirectly by way of amendment of the MLRs. It is reasonable, however, that the FCA should have similar powers *in relation to the prevention of financial crime* across all the firms it supervises under the MLRs.

54. In your view, would the expansion of the FCA's supervisory powers in the ways described above Annex 1 firms allow the FCA to fulfil its supervisory duties under the MLRs more effectively? Please explain your reasons in respect of each new power.

55. **In your view, what impacts would the expansion of the FCA's supervisory powers in the ways described above have on industry and the FCA's wider supervised population, both in terms of costs and wider impacts? Please provide evidence where possible.**

56. **In your view, what impacts would the expansion of the FCA's supervisory powers in the ways described above have on the FCA, both in terms of costs and wider impacts? Please provide evidence where possible.**

56. Do you agree with the overarching approach of tailoring the provisions of the FTR to the cryptoasset sector?

We are supportive of the general approach, but note that several terms will need amendment in order to avoid the application of payment services law to transactions in cryptoassets. These terms include:

- 'Transfer of funds,' which should become 'transfer of cryptoassets;'
- 'Payer,' which should become 'originator;'
- 'Payee,' which should become 'beneficiary;' and
- 'Payment service provider,' which should become 'cryptoasset service provider.'

57. In your view, what impacts would the implementation of the travel rule have on businesses, both in terms of costs and wider impacts? Please provide evidence where possible.

We do not have data on costs, but provide information on challenges that implementation of the requirements poses below.

58. Do you agree that a grace period to allow for the implementation of technological solutions is necessary and, if so, how long should it be for?

There are currently no formal processes in place for a technological solution, although work on this is ongoing informally in the US. We estimate that the earliest at which a solution may be available is in 2023. Given this estimated timeline and the fact that different blockchains may require different solutions, we urge caution in bringing the FTR requirements into effect before 2024. It should be noted that manual compliance with the FTR without a technological solution is not a feasible option, as it would not be scalable given the number of different tokens in existence.

Use of provisions from the FTR

59. Do you agree that the above requirements, which replicate the relevant provisions of the FTR, are appropriate for the cryptoasset sector?

We would like to highlight 4 areas for comment:

1. Exemptions from scope: The consultation does not detail the exemptions from scope that will be available to cryptoasset service providers. In particular, the exemptions relating to

- Instruments that are exclusively used to pay for goods or services (article 2(3));
- Transfers that involve the payer withdrawing cash from the payer's own payment account (article 2(4)(a));
- Transfers to a public authority as payment for taxes, fines or other levies (article 2(4)(b); and
- Transfers where both the payer and the payee are payment service providers acting on their own behalf (article 2(4)(c))

are also relevant to cryptoasset service providers. Given the similarity of some cryptoasset to e-money products, these exemptions should also be extended to cryptoasset service providers.

2. Information requirements: The table on page 31 of the consultation sets out information requirements that go beyond those currently required by the FTR. Most notably, what are currently alternatives in the list of information required by the FTR on the payer/originator ("the payer's address, official personal document number, customer identification number or date and place of birth" (article 4(1)(c))) have been set out as separate requirements, namely (a) address, (b) personal document number, (c) customer identification number or date and place of birth. It is unclear whether this rise in the compliance burden has been intentional or not, but it would result in the need to collect additional documentary evidence in order to verify these different items of information. For this reason, we suggest reverting to the requirements as they are currently stated in the FTR.

3. Including information with the transfer: Specific provision should be made for cases in which it is not possible to include the information on the payer and payee or attach it directly to the cryptoasset transfer.

4. Monitoring for required information: The consultation document appears to impose an additional requirement on cryptoasset service providers to match information on the beneficiary received with an incoming transfer to information already held on file for that beneficiary. Such a requirement is implied by the text in paragraph 6.15 of the consultation document and may have merit in order to prevent fraud, but it is not part of the FTR. While the FTR in article 7(3) imposes a requirement to verify the accuracy of the beneficiary information received, this requirement is expressly disapplied by article 7(5) in cases where the identity of the beneficiary has already been verified. The requirement therefore only applies where the beneficiary is not already an account or wallet holder, in which case it mirrors the identity verification requirement. Checking whether the information on the beneficiary matches that held on file is not a

requirement under the FTR, which merely requires checking for missing, incomplete or meaningless information (for a confirmation of this understanding, also see paragraphs 1.10 and 1.22 of part III of the JMLSG guidance and paragraphs 61-62 of the EBA's guidelines under article 25 of the FTR).

Provisions specific to cryptoasset firms

60. Do you agree that GBP 1,000 is the appropriate amount and denomination of the de minimis threshold?

Transfers in cryptoassets should be treated equally to other transfers, particularly given the new AML regime that cryptoasset service providers are subject to, which will reduce the inherent risk of cryptoasset transfers. A threshold (both for the transmission of information and the verification thereof) will also greatly reduce complexity for low-value transfers. We therefore agree that this is the appropriate amount and welcome the denomination in pounds sterling.

61. Do you agree that transfers from the same originator to the same beneficiary that appear to be linked, including where comprised of both cryptoasset and fiat currency transfers, made from the same cryptoasset service provider should be included in the GBP 1,000 threshold?

We would like to draw your attention to the volatility in the value of non-asset-backed cryptoassets and the difficulties this may cause in identifying linked transactions that exceed the threshold. While we agree that fiat currency transfers should be included in any assessments of links, it is unclear how cryptoasset service providers should take account of the value of historic transactions when deciding whether a current transaction exceeds the link threshold.

62. Do you agree that where a beneficiary's VASP receives a transfer from an unhosted wallet, it should obtain the required originator information, which it need not verify, from its own customer?

The approach taken at EU level is the exclusion altogether from the scope of the travel rule of any transactions that involve an unhosted wallet, and we think this is a preferable approach. Requiring customers to provide identifying information related to unhosted wallets could lead to inaccurate records, given that the information will not be verified. Such information would be of little use to law enforcement and may even hinder investigative efforts. It might be more beneficial for investigation purposes to require firms to record available data relating to originator/beneficiary wallets than to ask them to record information that may not be accurate or may indeed be misleading. Such a requirement could also potentially deter customers from using regulated firms in favour of unhosted wallets. We would encourage further assessment of the risks of transactions involving unhosted wallets, as it is not immediately apparent that such transactions uniformly present a higher risk.

63. Are there any other requirements, or areas where the requirements should differ from those in the FTR, that you believe would be helpful to the implementation of the travel rule?

Paragraph 6.17 of the consultation document mentions a cyrptoasset service provider's ultimate obligation to reject future transfers from a non-compliant provider or terminate its business relationship with that provider. Please note that for cryptoasset service providers, it is neither possible to reject transactions nor to identify the provider from an incoming cryptoasset transfer and thus restrict incoming transfers to compliant providers. Therefore, this requirement should be amended to require cryptoasset service providers to either return the transaction to the originator if the required information has not been provided even after repeated promptings or report a consistent failure to comply to the competent authority while holding the transferred cryptoassets without making them available to the beneficiary, pending review by the competent authority (the approach taken at EU level).

List of EMA members as of October 2021

AAVE LIMITED
Account Technologies
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
American Express
ArcaPay Ltd
Azimo Limited
Bitpanda Payments GmbH
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crosscard S.A.
Crypto.com
Curve
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
ePayments Systems Limited
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
Modulr FS Europe Limited
MONAVATE
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Europe Limited
OFX
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Oxygen
Park Card Services Limited
Paydoo Payments UAB
Paymentsense Limited
Payoneer
PayPal Europe Ltd
Paysafe Group
Plaid
PPRO Financial Ltd
PPS
Remitly
Revolut
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Snowy Pay Ltd.
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
Vitesse PSP Ltd
Viva Payments SA
Vivid Money Limited
Weavr Limited
WEX Europe UK Limited
Wirex Limited
Wise
WorldFirst
WorldRemit LTD