connecting the future

Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022

HM Treasury (HMT)

21st October 2021

Response from The Payments Association

Abstract

This paper sets out the Payment Association's response to the HM Treasury's consultation: ***Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.*** *It contains recommendations on how to ensure the UK's payments industry continues to effectively tackle and prevent financial crime.*

21st October 2021

Introduction – Tony Craddock, Director General, The Payments Association

The Payments Association welcomes the opportunity to contribute to HM Treasury's:

1. Call for Evidence (CfE) - review of the UK's AML/CFT regulatory and supervisory regime and
2. Consultation on Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (information on then Payer) Regulations 2017 Statutory Instrument 2022

Our community's response contained in this paper reflects views expressed by our members and industry experts. As The Payment Association's membership includes a wide range of companies from across the payments value chain, and diverse viewpoints across all job roles, this response cannot and does not claim to represent the views of all members fully.

We are grateful to The Payment Association's members and the experts they have recommended to us, who have contributed to this response which has been drafted by Jane Jee, a consultant, and Project Financial Crime Lead for The Payment Association. We hope it advances our collective efforts to ensure the UK's payments industry continues to be progressive, world-leading and secure, and effective at serving the needs of everyone who pays and gets paid.

Tony Craddock
Director General
The Payments Association

connecting the future

Introduction – Jane Jee, Project Financial Crime Lead, The Payments Association

The Payments Association (TPA) is pleased to have the opportunity to respond to the HMT's

1. Call for Evidence (CfE) - review of the UK's AML/CFT regulatory and supervisory regime and
2. Consultation on Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (information on then Payer) Regulations 2017 Statutory Instrument 2022 (Consultation)

The Payments Association (TPA) represents a broad range of organisations; many members are regulated persons under AML legislation i.e. established banks, Challenger banks and Fintechs (including Electronic Money institutions and Authorised Payment Institutions). TPA also has card scheme members and members who are vendors into the payments market, some of which are RegTech companies offering solutions to help prevent financial crime. At present these companies do not fall to be regulated under AML legislation. TPA may be one of the few responders to the's CfE which represents such AML technology (Regtech) firms. Sophisticated criminals know how to bypass many of the basic AML controls used today and have identified the vulnerabilities of detection systems implemented by financial institutions. The systems being used to fight back – a combination of technology and human expertise - need to continually evolve and aim to be one step ahead of the criminals who ruthlessly exploit any weaknesses and use the latest technology to achieve their ends.

TPA has been provided with a copy of the UK Finance response to the CfE and Consultation. We agree with the statement that the private sector expenditure on preventing financial crime could be more effective if directed towards high value, threat focused activity.

Globally fraud and economic crime rates remain at record highs, impacting companies in more ways than ever. TPA recognises that there has been a long series of leaks uncovering abuse of the world financial system by the rich and powerful. The latest of these is the Pandora Papers which reveal the names and secret dealings of politicians and world leaders. The Papers have caused increasing criticism and scrutiny of such dealings and more governments around the world are pledging investigations in the wake of the Papers which constitute the biggest-ever offshore leak.

Against this backdrop, HMT, in reviewing AML laws in the UK, has an opportunity to help prevent financial crime which is so damaging to the UK's economy and financial stability as well as its global reputation as the place to locate a business. We would, like UK Finance, encourage HMT to look more broadly than just the MLRs. We agree that there are tensions between existing legislation and guidance which has led to a lack of clarity across the regulated sector.

Whilst the TPA supports a risk-based approach there needs to be more emphasis on outcomes and this will only be achieved with clearer more effective leadership and clear responsibility. Supervision of ML/TF is currently unnecessarily fragmented. We support the call made by UK Finance for a single leader with ML/TF responsibility across the public sector and a more developed threat assessment as well as a set of clear objectives and principles for all supervisors. Maintaining the integrity of the financial market is a key objective for the FCA – this is interpreted as requiring firms to maintain effective systems and controls to prevent money laundering and terrorist financing. None of the AML supervisors is mandated to consider how technology might be deployed to reduce the cost and increase the effectiveness of ML/TF controls. An overarching obligation on supervisors would spur on the use of relevant effective technology and potentially accelerate progress.

The government's ambition should be for the AML/CTF sector to be at the forefront of innovation and technology in the same way as it has that ambition for the payments sector. If we are to foster a vibrant payments market in the UK, TPA believes that we should ensure that financial crime is not an area for firms to compete in but rather to collaborate and share relevant data. It is critical that the right data (especially live intelligence) is available to regulated firms of all sizes to make the appropriate risk assessments of prospective customers and monitor them in a robust manner. Currently smaller financial institutions bear an unfair cost and effort burden to comply with AML requirements. This means that the UK is not able to realise the full benefits of the digitisation of the economy and take advantage of the opportunities it represents (as stated in the Kalifa review).

The UK has an opportunity to be a world leader in the AML/CTF field. The public sector has a vital role to play in enabling the right framework and data availability so that private sector can play in turn its part to prevent financial crime. The public sector controls many data sources which are vital to preventing financial crime: examples are reforms to Companies House (so that the beneficial ownership of companies is transparent and abuse of companies is prevented) the DCMS framework on digital identity, the SARs reform programme and reform of the law on corporate liability for economic crime should all be expedited. The level of knowledge and understanding of ML/TF challenges and available efficiencies among supervisors must be increased. FCA AML focused Techsprints have gone some way to achieve this – the FCA noted "Profound and rapid learning for regulators, firms and others on the application and impact of emerging technology" [i] but overall such initiatives have produced few tangible anti financial crime results. Innovative private sector firms, even if able to find the time and resources to participate, cannot simply donate their intellectual property which would stifle their growth and investment. Arguably the FCA is the wrong body to facilitate such activities given their need to be technology/solution provider neutral and their role as AML supervisors.

We would also echo the request made in the UK Finance response – given that the AML/CTF regime relies on a significant amount of processing (sharing/analysing etc) of personal data in order for it to function, that guidance should be issued on interaction between the regime and the requirements of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA). We agree that understanding the interplay of the two sets of requirements (GDPR and MLR) is key to ensuring necessary and proportionate application of the MLRs, to ensure we combat financial crime in a fair, transparent and accountable way. TPA members also need clear guidance on how to navigate between the two regimes, and the TPA would welcome clarity on the retention schedules set out in the current MLRs - they are extremely difficult to understand and implement.

Chris Hemsley - PayExpo Payments Leaders' Summit on regulation of Open Banking, payment competition and fraud in interbank payments - 5 October 2021

But, today, I'd like to focus on three groups: those who are currently falling well short of where we need to be.

First - we need social media firms to step up and make it hard for criminals to seek out their victims using their platforms. Something that, as the FCA has highlighted, actually makes social media firms money from the adverts criminals' place.

Second - we need to see action from payment firms who have not signed up to the Contingent Reimbursement Model and who are not offering similar levels of protection. You need to protect your customers.

And third – to those banking these criminals, however inadvertently - we need to know where the funds are going. Many of the sending banks are stepping up their efforts – but is there enough focus on where the funds are received?[1]

Finally TPA would draw attention to the independent Taskforce on Innovation, Growth and Regulatory Reform report was released on June 16, 2021 to set out a near-term vision for the future of UK regulation.
The report does not specifically address payment service providers (PSPs) in full, with the exception of a proposal for reduced AML burden on account information services providers (AISPs) and payment initiation services providers (PISPs), currently in consultation and PSPs' role in facilitating retail central bank digital currency (CBDC) payments.
The two key changes outlined throughout the report are:

1. The UK's move from codified law towards principles-based common law to increase competition both domestically and internationally.

2. The drive for the establishment of a framework that supports and nurtures digital innovation.

[1] https://www.psr.org.uk/news-updates/speeches/speeches/pay360_chris-h_oct-2021/

The report proposes the UK could implement a framework that supports leadership in fintech (Proposal 5) as follows:

- Proposal 5.1: Mandating an expansion of open banking to open finance. (note: The Kalifa Review of UK Fintech was noted and praised in the report.)

- Proposal 5.2: Increasing competition in the banking sector by adopting a graduated regulatory approach for challenger banks.

- Proposal 5.3: Reducing anti-money laundering (AML) burdens on open banking/fintech services.

- Proposal 5.4: Accelerating plans for a UK CBDC to launch a pilot in 12 to 18 months.

The report also proposes (Proposal 1.5) to continue the use of digital sandboxes and to optimise their use whereby:

- Regulators should be able to review and share the data and the lessons they learn from data with other relevant bodies.

- Sandboxes should be digital by default. Previously, sandboxes have been established in silos and the data has not been readily available in electronic format or for others to review.

Jane Jee
Project Financial Crime Lead
The Payments Association

Contents

EPA Responses

The section below corresponds to the numbering as listed in Annex B 'List of Consultation Questions'

AISPs (Account Initiation Service Providers) and PISPs (Payment Initiation Service Providers)

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

A PISP is a conduit for instructions between a biller, a payer and their banks. A PISP, to be operating, will have been, and remains, authorised and regulated by the FCA. As part of original authorisation, the FCA assesses a PISP's business case, security provisions, risk assessments, shareholders, and executive for fitness to act purposes. A PISP does not provide a potential Money Launderer or Terrorist Financer with any capabilities or tools that would allow them to launder money or finance terrorism any more easily than using the existing process of Faster Payments.

A business submits a payment request to their chosen PISP, with whom they have a contract (in some cases they accept the PISPs terms and conditions online) the PISP then sets up this payment in the potential payer's bank account, where the payer is required to authorise payment for money to transfer in accordance with the businesses and payer's instructions and consent.

Today, if a business or consumer wishes to be paid by a Faster Payment bank transfer, they provide their payer with a sort code, account number, and their account title, together with the amount and any payment reference they wish to see on the transfer. This information may be passed on paper, by email, electronic message or by voice call. The payer then uses their internet or mobile or telephone banking service to set up and send the payment, under the protection of the sending bank's SCA. ML and TF oversight of this process is undertaken through the two parties' banks and for certain high-risk types of business (e.g. estate agents) directly via the business collecting payment. Each bank has visibility of their customer transactions and the best opportunity to monitor for ML/TF issues.

A PISP transfers money from one account held with an authorised bank over which there are general account opening AML obligations and KYC stipulations, to the receiving bank with equivalent obligations. Banks are in the position of being able to see all account activity of their customers, unlike a PISP. A bank is the party best placed to discern any unusual activity. A bank is the party which should carry out KYC checks on their potential customers and satisfy themselves that they are not opening an account for a fraudster.

The Payments Association consider that requiring the Payment Service User (PSU) to undergo any CDD, even using innovative means such as scanning a passport with a phone, would be enough to dissuade that customer from proceeding to use the open banking service. In e-commerce, for example, it is very unlikely that a customer would consider uploading their passport just so they could use PIS to pay, as opposed to using their debit card, which wouldn't require any documentation to be provided. 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'.

However, we note that the definition of 'customer' in the EBA sector guidelines creates some ambiguity regarding what action PISPs should take around occasional transactions. Our view

is that if the PISP is treating the payee as the customer, with which it has a business relationship, occasional transactions would be irrelevant, as they are by definition, 'transactions which [are] not carried out as part of a business relationship.

The issue is also being addressed with a draft provision in the new EU regulation on AML/CFT. Recital 34 states that:
"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'
.
A payer's (the party the subject of this consultation) primary relationship is with their bank. Banks are already under obligations to carry out adequate AML/KYC checks on their potential customers before opening an account for them and to continue appropriate ongoing fraud checks. It is a payer's bank that has the fullest picture of what payments in and out are usual for a particular customer. Where a party such as this in such a position, has the primary relationship with the customer and is already under an obligation to carry out checks, not only does it not give any further AML/TF mitigation to require a 2nd party to duplicate such checks, but it may also serve to encourage less vigorous checks by the primary party (bank) in the first place.

Please also see our response to Q4 below.

Finally, according to the **Taskforce on Innovation, Growth and Regulatory Reform report (p. 44)**, open banking services that provide significant benefits to consumers, such as AISPs and PISPs, have sufficiently low or virtually non-existent money laundering risks associated with them.
For consumers to take up open banking, the report suggests:
Removing duplicative AML/know your customer (KYC) checks for AISPs and PISPs (that are already performed by banks). Reducing unnecessary costs for fintech businesses Improving the consumer journey as a result

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

PISPs have to undertake a risk assessment of the impact that their service can have on ML and TF as part of their authorisation process and on an ongoing basis. Beyond normal requirements for record keeping of payments transactions enabled by the PISP's service and processes to ensure that payers know who they are paying, and relevant checks (eg email and account title verification) on the party requesting payment, PISPs do not currently see a particular compliance burden. If there was a general view that PISPs had to duplicate the ML and TF obligations and processes of the banks directly involved in these payments on the payer, then PISPs compliance costs would be increased significantly. It would require altering the PISPs technology at a platform level and would make use of the service costly and unattractive. The costs of hiring more staff and building more services would not assist in preventing financial crime and would divert funds which could be better spent creating innovative services to compete with incumbent payment service providers, and directing funds to eg the receiving of fraudulent money by the receiving bank, as per Chris Hemsley's comment referenced in our introduction.

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

In order to ensure that PISPs can provide a seamless experience at the checkout for retail payments (equivalent to cards), it needs to be ensured that PISPs who provide an open banking payment method on a merchant's website (and may have never come across a particular PSU before), do not need to stop a payment flow at the check-out in order to ask a PSU for KYC/ CDD. If this were to be the result, it would undoubtedly lead to customer's abandoning purchases and not using open banking as a payment method again. It would be much slower to use PIS than to use cards.

If PISPs (in addition to Account Servicing PSPs) were required to KYC all payers, this would stifle this innovation and undermine the innovation envisaged in PSD2. It would place a greater regulatory burden on PISPs than ASPSPs who do not need to validate where payments come from into their customers' accounts via Faster Payments. If PISPs were required to KYC all payers, then these services could only be used by payers who had proactively registered for each PISP service, going through a KYC process not unlike that required to open a bank account at an ASPSP. This will fundamentally undermine most PISP customer propositions, preventing PISPs bringing competitive pressure to bear on banks. Given that all payers using PISPs must make payments from UK ASPSPs, and to have an account with an ASPSP they must have gone through a KYC process to open that account, requiring this to be duplicated by the PISP adds no benefit in ML/TF terms at a large cost.

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

AISPs aggregate information they do not transfer funds. The Payments Association considers that AISPs should not be obliged to screen customers under AML legislation. In addition, for the reasons set out above The Payments Association considers that the ML/TF risks presented by PISPs are very low and should therefore also be exempted from the regulations.

BPSPs (Bill Payment Service Providers) and TDITPSPs (Telecom, Digital and IT Payment Service Providers)

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.

Going back to first principles, it is disproportionate for BPSPs to have to comply with MLRs, since, by definition, others in the payment chain will also be doing such checks. Applying MLR regulations to such entities would also stifle innovation and make it harder for new companies to innovate in the presentation of payment options to consumers. The same can be said about TDITPSPs.
Moreover, the risk associated with such firms are also very low. The services whose purchase they facilitate are simply not a target for Money Launderers. Getting credit on your phone bill, or a sword in a fantasy game is not a way to finance terrorism.

The Payments Association believes that the guiding principle should be to be proportionate in AML/ATF regulation. The imposition of the MLRs in these circumstances have a real cost and questionable benefits.

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?

The Payments Association does not believe that there would be any increased direct costs or other potential adverse impacts if BPSPs and TDITPSPs were to be taken out of scope of the MLRs.

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?

   It seems likely that the costs and administrative burden on both HMRC and registered businesses would be reduced. However there are no accurate figures available on the number of such PSPs and therefore it is difficult to know the extent of the reduction in such costs and burden.

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

   The Payments Association does not believe there would be any wider impacts.

Art Market Participants

9. In your view, what impact would the exemption of artists selling works of art, that they have created, over the EUR 10,000 threshold have on the art sector, both in terms of direct costs and wider impacts? In your view is there ML risk associated with artists and if so, how significant is this risk? Please provide evidence where possible.

   The UK National Risk Assessment (NRA) 2020 covered AMPs for the first time. Art businesses were only previously captured by the Money Laundering Regulations (MLRs) if they were in scope as a High Value Dealer (HVD). The 2020 NRA assessed AMPs separately to HVDs as their risk profile and their definition differs. AMPs are currently assessed as high risk for money laundering and low risk for terrorist financing. The UK NRA reports the art market to be attractive for money laundering because of the ability to conceal the art's beneficial owners, the final destination of art, the wide-ranging values involved, and the size and international nature of the market. It adds that it is too early to fully assess the effectiveness of new mitigations in place by AMPs under the Money Laundering Regulations.

   The Payments Association is not in a position to comment on the impact of the exemption on the art sector.

10. As the AML supervisor for the art sector, what impact would this amendment have on the supervision of HMRC? Would the cost to HMRC of supervising the art sector decrease? Are there any other potential impacts?

    Given the low number of artists selling work of this nature there is not likely to be a significant impact upon the supervision of HMRC. We consider this change is "tinkering at the edges" and will not significantly increase HMRC's supervisory capability.

11. In your view, does the proposed drafting for the amendment to the AMP definition in Regulation 14, in Annex D, adequately cover the intention to clarify the exclusion of artists from the definition, where it relates to the sale and purchase of works of art? Please explain your reasons.

    The proposed drafting amendment will adequately cover the exemption of the specified body of artists.

12. In your view, should further amendments be considered to bring into scope of the AMP definition those who trade in the sale and purchase of digital art? If so, what other amendments do you think should be considered?

    The Payments Association notes the risks of ML set out in the article below and urges HMT to ensure that those who trade in the sale and purchase of digital art are brought within the AMP

definition**https://www.fountaincourt.co.uk/wp-content/uploads/Edition-1-Commentary.pdf** SARs (Suspicious Activity Reports)

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?

We agree with UK Finance that the provision of individual SAR information by reporters would not necessarily allow enhanced performance of supervisory functions as the NCA is best placed to assess this information. It is also likely that supervisors would not be consistent in their use of this power or the conclusions they draw from the results.

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?

It can be argued that the current text contained within regulation 66 is sufficient to allow supervisors to access the contents of SARs in that it covers the ability for a supervisor to require a regulated entity "to (a) provide specified information, or information of a specified description; or (b) produce specified documents, or documents of a specified description". We believe that there may be circumstances when a supervisor's role could be enhanced by sight of the contents of SARs.

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?

This is difficult to generalise about - it could potentially help in certain circumstances.

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 agree with UK Finance that the value of SARs should be assessed against adherence to the criteria set out by NCA guidance and with the benefit of a complete view of information provided through multiple SARs that, taken together, may provide the NCA with actionable intelligence on specific targets.

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.

We agree with UK Finance that this will depend upon the way the proposed change is implemented and we agree that any such change should seek not to place any greater burden on the private sector.

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.

Our concern is that there may be a series of SARs relating to one entity and the wrong interpretation could arise if only one or some of such SARs are analysed.

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?

The Payments Association is supportive of the requirement to clarify the scope of activities that define credit and financial institutions, and to align the MLRs with FSMA if it helps to foster harmonisation. However, care must be taken to review the additional companies which may be brought into scope by any change. I some cases this may stifle competition which would not be desirable and present very little gain.

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.

TBA

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

The Payments Association consider that more guidance should be available to smaller and start-up firms where they have questions as to whether a particular activity is within scope. We agree with UK Finance that those sectors that bring fraud and/or money laundering risk into the system, (for example unregulated small legal and accountancy firms, as well as social media and telecoms companies) should be brought into scope of the MLRs.

It is clear that many third-party providers to the financial services sector (including many Reg-Tech companies) do not fall to be regulated under AML legislation but it would probably help such companies and certainly give greater confidence to the financial institutions who use them, or would like to use them, if there was a system of certification of their business. This has been mooted in the past and it should be carried out by an independent body and not one dominated by the larger financial institutions.

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.

We consider the relevant persons brought into scope are best placed to respond on this.

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.

An expansion in the remit of the FCA could adversely impact their supervisory effectiveness which in relation to their financial crime remit would be negative.

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?

Proliferation Financing Risk Assessment

We agree with the responses provided by UK Finance to the following questions 25-30.

25. Do you agree with the proposal to use the FATF definition of proliferation financing as the basis for the definition in the MLRs?
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.
27. Do relevant persons already consider PF risks when conducting ML and TF risk assessments?
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.

Formation of Limited Partnerships

Extension of the application of the term TCSP to cover all forms of business arrangement (that are registered with Companies House)

31. Do you agree that Regulation 12(2)(a) should be amended to include all forms of business arrangement which are required to register with Companies House, including LPs which are registered in England and Wales or Northern Ireland??

    Yes. Further consultation is needed to be able to respond to the questions which follow in this section 4.B

32. Do you consider there to be any unintended consequences of making this change in the way described? Please explain your reasons

    No response

33. In your view, what impact would this amendment have on TCSPs, both in terms of costs and wider impacts? Please provide evidence where possible.

    No response

34. In your view, what impact would this amendment have on business arrangements, including LPs which are registered in England and Wales or Northern Ireland, both in terms of costs and wider impacts? Please provide evidence where possible.

    No response

Extension of the term "business relationship" for services provided by TCSPs

35. Do you agree that Regulation 4(2) should be amended so that the term "business relationship" includes a relationship where a TCSP is asked to form any form of business arrangement which is required to register with Companies House?

    We agree that Regulation 4(2) should be amended to include where a TCSP is asked to form any form of business arrangement required to register with Companies House.

36. Do you agree that Regulation 4(2) should be amended so that the term "business relationship" includes a relationship where a TCSP is acting or arranging for another person to act as those listed in Regulation 12(2)(b) and (d)?

    Yes

37. Do you agree that the one-off appointment of a limited partner should not constitute a business relationship?

    Yes – however we agree with UK Finance that further study of the practical impact of this requirement would be beneficial.

38. Do you consider there to be any unintended consequences of making these changes? Please explain your reasons.

    No response

39. In your view, what impact would this amendment have on TCSPs, both in terms of costs and wider impacts? Please provide evidence where possible.

    No response.

40. In your view, what impact would this amendment have on business arrangements, including LPs which are registered in England and Wales or Northern Ireland, both in terms of costs and wider impacts? Please provide evidence where possible.

    No response

Reporting of Discrepancies

We agree with UK Finance's comment that this consultation and the Call for Evidence include a number of proposals that directly impact on Companies House reform. We are supportive of reforms to Companies House but consider that a fair balance needs to be achieved between what Companies House is obliged to check and the burden placed upon relevant persons. We agree with UK Finance that this issue needs to be part of a more effective whole-system response to economic crime.

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 Payments Association is prepared to support the obligation being ongoing provided that Companies House have the resources to follow up on such discrepancies in a timely manner. We think the phrase "should reasonably have become aware of" is vague and too open to interpretation. Also, what constitutes a discrepancy needs to be clarified - what is material versus a trivial discrepancy. Once Companies House has been reformed so that Directors' identities are checked at registration, directors are obliged to file updates to all company information and the penalties are made significant and enforced, we hope that the reporting of discrepancies will become less of a burden on the private sector.

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

    The responsibility for filing accurate, timely information should sit with the companies themselves and Companies House as the owner/controller of the register. Relevant persons need to be able to rely on the accuracy of the data.

The definition of Beneficial Owner under the MLRs and Persons with Significant Control (PSCs) are not aligned. The registration requirements for PSCs may include legal entities and not a natural person/individual. These issues need to be addressed before the current obligations are expanded.

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

Documents filed at Companies house should be subject to rigorous checking by those filing them – for example subject to the four eyes test so that two members of the relevant company have to check filings. Companies House need to use appropriate technology to reject inaccurate or misleading filings as well as human judgement. Possibly Companies House penalties should be altered to reflect the size and nature of the legal entity that is filing information. Any Company making a filing which is deemed to be deliberately misleading should be subject to higher sanctions.

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?

If built on top of the proper reform of Companies House this change should be manageable by relevant persons whose costs in checking Companies House data will be reduced.

Disclosure and Sharing

We agree that high quality information and intelligence sharing across both the public and private is a key tool in the fight against financial crime. To achieve this end, we need clearer guidance on the conflict between data protection and sharing personal information to prevent financial crime so that regulated persons can share appropriate relevant data with more confidence.

analysis and remediation of the disproportionate burden (cost and effort) placed on smaller regulated companies that do not have the same access to relevant information and intelligence to prevent fraud and ML as larger ones. Some sources charge an upfront fee instead of pay per use. It means smaller companies suffer a higher level of fraud and abuse by criminals.

It is not only the public sector who need to share information – consideration should be given to how companies that offer innovative AML/fraud solutions (RegTechs) and that cannot be classified as relevant persons can obtain access to such data.

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

Possibly – however we would like clarification on how and for what purpose BEIS would use such intelligence and information before expanding the scope of Regulation 52.

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

We agree with UK Finance that OFCOM and DCMS should be considered for inclusion in the scope of Reg 52 if our suggestions on identifying new areas where risk is introduced are accepted.

We would reiterate that all regulated Fintechs and (appropriately certified?) RegTechs that supply AML/anti-fraud data need better support to obtain the same information as banks – this should not be an area for competition but collaboration.

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, this would seem a sensible amendment subject to appropriate wording to protect data privacy.

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.

The expansion of Regulation 52 may have an impact on data privacy, so that information shared by supervisory authorities should be on a need-to-know basis and the relevant firm should be informed when, and the extent to which, information is being shared.

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.

We can see that this may increase costs, but we have no relevant information to provide beyond this observation. Given that a number of supervisors are not operating effectively (as noted in OPBAS latest report [2] and have conflicts in terms of being member organisations we hope that the review will seek to address these matters.

50. 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?

The PA does not have a view on this point but, as stated above , broader consideration of information sharing powers on economic crime is required.

Information Gathering

We agree with the points made by UK Finance in response to questions 51-55

51. 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.
52. 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.
53. 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.
54. 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.
55. 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.

[2] https://www.fca.org.uk/publication/opbas/supervisory-assessments-progress-themes-2020-21.pdf

Transfers of cryptoassets

Revision of Regulation 2015/847/EU: the **proposal** to update **Regulation 2015/847/EU** on information accompanying transfers of funds and certain crypto-assets (recast) aims to expand the regulation's scope, which currently only applies to the transfer of funds, which are defined as "banknotes and coins, scriptural money and electronic money" to include crypto-asset transfers.

Specifically, it introduces obligations for these providers to gather and make available to the relevant authorities data related to the originators and beneficiaries of the virtual assets transfers, provided by Financial Action Task Force (FATF) **Recommendation 16**, which sets out wire transfer requirements, known as the "travel rule".

The German Federal Ministry of Finance published an ordinance on increased due diligence in the transfer of crypto values (**Krypto Valet Transfer Ordinance - KryptoTransferV**) based on Section 15(10) sentence 1, number 1 of the Money Laundering Act (GwG), which implements the standards of the FATF "travel rule"), which came into force on October 1, 2021.

The approach to implementation

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

The FTR provisions can be applied to the crypto asset sector but the key area that requires attention is tailoring. It is well known that to send or receive crypto assets require very little information to be sent/transmitted or received. To gather information such as that proposed within the Travel Rule is something that will be completely new to the industry as a whole. It is certainly a welcomed approach as "knowing your transaction" is fundamental, however the approach must be tailored on a risk-based approach.

Although standardisation is warranted, in-country transfers below GBP 1,000 (e.g UK to UK) should require a more simplistic form of information being transmitted such as first and last names plus date of birth. The risk here can be rated as a lower risk dependent on business set ups and plans. Through appropriate UK regulation of firms, at the authorisation stage, a have to prove they are fit and proper as well as provide their business plans and controls in place.

Furthermore, regulation for the crypto asset industry must be tailored and implemented carefully to maintain the integrity of the financial system. Indeed, heightened regulations will remove bad actors from platforms, however, many more platforms that are unregulated will appear whereby bad actors will decide to move their crypto assets through. A balancing act here is required and by requiring increased sender and beneficiary information to be shared, it increases the scope of unregulated firms carrying out business leading to illicit behaviour and activity.

Comparing transaction monitoring in the traditional fiat sector to that of the crypto-asset sector, although more originator and beneficiary is captured within fiat. Through blockchain transaction monitoring solutions, there is no issue with transparency. At any given time, through investigation, crypto asset movement can be tracked from one exchange or service to another with the total amounts moving. As a result of this, the belief is that crypto asset firms that operate within regulations, are operating in a more transparent manner than that of the traditional fiat services. Adding further layers of information on originator and beneficiary will increase this without a doubt and the provisions of the FTR should certainly apply to crypto assets but tailored on a risk-based approach dependent on volumes, countries transferred to and from, values of crypto assets in fiat at time of transaction and other factors that may be inherent.

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.

The cost will be great as many firms may not be large enough to scale up their technology to implement the travel rule. VASPs essentially require an electronic means of communicating with one another to transfer the recommended information. A company such as Coinbase will be able to afford the technology infrastructure, development resources required and the costs associated whereas a firm that doesn't intend to transact thousands in volume a month but just merely hundreds may not be able to afford such resources.

Intervening in transactions is not feasible, as on the blockchain these transactions are being verified and validated. At a crypto asset transaction level, transactions can be monitored and tagged with illicit activity if required, but the crypto-asset can also be frozen. A full intervention is not practical.

A key area is the due diligence carried out by firms. If documents and information have been collected, which more firms do, then this should mean that less information needs to be transferred. It is almost a staple now that crypto asset firms request a copy of in date ID, proof of address that is government issued and no older than 3 months, a liveness check as well as sanctions screening is implemented. These types of controls should be regulated and required by all firms meaning less data needs to be shared as this will result in a more trustworthy network of crypto firms as they would need to comply with capturing these documents and information.

As mentioned earlier, a tailored approach is necessary as this is new in the crypto asset area (Travel Rule). Imposing data sharing may open the industry up to illegal unregulated exchanges not only in the UK, but globally. Although these exist at present, this could become more prevalent and burdensome.
It is reasonable to expect that the cost and implementation timelines will be significant. The UK Government should consider a staged approach to implementation and technical guidance for the industry that is interoperable with the global standards.

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?

A grace period is of fundamental importance. After regulations have been enforced, a grace period of one year should be implemented. The reason for this is to allow the technologies to be imbedded within the compliance regime of firms and to ensure they are able to share and store data appropriately. As an example, the Senior Managers & Certification Regime had a year or more to implement. As we are considering technology for the Travel Rule to be successful, a period of one year would be recommended as this would allow the market to also mature.

Use of provisions from the FTR (Funds Transfer Regulation)

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

We agree on this point. However, once again, it should be for firms to have appropriate risk assessments in place as well as controls and procedures to implement the requirements.

Additionally, it should not be defined as to which information should be shared. Rather, it should be best practice. If a firm is regulated, it means it must be trusted by the regulator as they will have authorised the firm based on their application. As a result of this, they should be effectively governed and have appropriate oversight through thematic reviews, firm information requests and examinations where warranted.

Provisions specific to cryptoasset firms

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

Agreed. GBP 1,000 appears to be in line with the industry expectation and other regulatory requirements.

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?

Agreed.

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 Payments Association agrees with the response given to this question by UK Finance.

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?

Not at present.