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

UK Finance Response

UK Finance is the collective voice for the banking and finance industry. Representing around 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

We welcome the opportunity to respond to this consultation, seeking to further strengthen the UK's Anti-Money Laundering (AML) regime through the introduction of amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs), to further reflect existing risks threatening the integrity of the UK's financial system.

In responding to this consultation, we are conscious of the parallel "Call for Evidence: Review of the UK's AML/CTF regulatory and supervisory regime". We have sought to align our responses as far as possible, as we see both as important in shaping the future approach to tackling economic crime in both the near and longer term.

As part of that, we have sought to set out in the Call for Evidence (CfE), the wider and more significant changes to both the MLRs and the broader ecosystem, that we believe are required. These changes would create a stronger, more effective system, that manages risk by allowing resources to be focused towards agreed threat priorities to protect the public, cut crime and catch criminals. We also believe these changes would support growth and access to banking, whilst ensuring all those responsible for bringing in and managing risk in the ecosystem play their part to tackle it.

In setting out those changes, we have sought to ensure that our proposed changes set out below in the Statutory Instrument (SI) are compatible with the aims in the CfE, to both reduce risk and support effectiveness and efficiency.

With that aim in mind, whilst we have responded to and commented on the proposals set out below, we were surprised at how limited the proposed amendments were. This is a significant opportunity to move quickly to make several limited but important changes that would considerably advance our collective ability to tackle financial crime, whilst also bearing down on low impact activity.

There are a number of additional areas where we believe the MLRs could be strengthened, through the introduction of clarificatory amendments which are not being explored through this consultation. Considering the focus on ensuring recalibration of low impact or prescriptive activity within the UK's AML regime, we encourage consideration of the amendments included under Annex A to realign obligations towards a more proportionate application of intended AML/CTF measures.

In addition, we are conscious that despite the focus in the CfE on identifying and removing low impact activity from the AML ecosystem, this consultation is exploring the introduction of this type of activity, in particular through the proposed extension of BO discrepancy reporting obligations. The consultation does not reference overlapping proposals being explored as part of Companies House (CH) reform, such as the proposal to extend the reporting obligation to cover directors. We consider it crucial that both sets of proposed changes are developed holistically, as part of ensuring recalibration of low impact activity, and to avoid a scenario where we are introducing proposals that will distract resource whilst delivering little to no AML/CTF benefit.

The proposals would benefit from being more joined up, as we are concerned, they seem to conflict with several strategic priorities in the Economic Crime Plan, including:

- Ensure the powers, procedures and tools of law enforcement, the justice system and the private sector are as effective as possible.
- Build greater resilience to economic crime by enhancing the management of economic crime risk in the private sector and the risk-based approach (RBA) to supervision.
- Improve our systems for transparency of ownership of legal entities and legal arrangements.

We would welcome further discussion on this issue to ensure we do not inadvertently introduce great inefficiencies and risk into the system.

However, whilst areas where we would have concerns, we would repeat previous comments to acknowledge both the ambition of HM Treasury on reviewing and considering the current and future MLRs, and the openness and transparency by which you have approached the process.

We recognise that this SI is an important part of a wider package of needed reforms, and we are looking forward to continuing to engage with you further on this and other issues. We thank you for the opportunity to respond to this consultation, and look forward to engaging further on the identified themes.

Please contact Aminah Samad at aminah.samad@ukfinance.org.uk for any further information.

Account Information Service Providers and 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?**

We believe that overall, the ML/TF risks presented by AISPs are low, as they cannot access funds and cannot access accounts to execute payments.

The potential ML/TF risks presented by PISPs are noted as being slightly higher than AISPs, due to their involvement in payment chains. This also leads to the potential risk of PISPs being able to move money quickly out of funds placed in accounts using third party access.

However, for both AISPs/PISPs, members note that the fraud risk is potentially high. This includes the potential for AISPs/PISPs to be abused as part of a money mule network, as well as abuse against their individual payment user. AISP services can also be compromised by criminals to enable fraud elsewhere, for example by using account information to impersonate the victim. PISP-initiated payments are harder for financial institutions to monitor due to the loss of customer data regarding device, geolocation and behavioural metrics.

While historically the amount of fraud identified in AISP/PISP relationships has been low, this has recently started to increase in line with growth in the use of Open Banking services. There have also been instances of disproportionately high fraud volumes in PISP-initiated payments targeted by social engineering.

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

There is a tension here between supporting competition – particularly around minimising regulatory burdens and ensuring there is the right framework for long term management of system risk – that will need careful consideration.

Members note that the money laundering (ML) risk is low for AISPs, and only slightly higher for PISPs – and so the regulatory requirements should be drawn accordingly. Even for PISPs, in terms of the ML/TF risk, it is assessed as no greater or less than other payment service providers (such as cards).

Many members also note that CDD is already conducted by a financial sector firm where the payer's account is held (in line with Payment Services Regulations and MLRs), so a PISP conducting CDD would be a duplication of effort, and it is difficult to see how this would materially alter risk. Some members note that it may be worth considering this further in the context of any developments in the use of Digital ID, such as if there is a central repository of CDD information.

The cost of complying with MLR requirements is significant for AISPs and PISPs – such as CDD components (Identification, Verification and Determination of Purpose of Relationship), for every payment made by any customer utilising the service without introducing friction to the payment journey.

Many members believe that the obligations imposed by the MLRs on PISPs have been a considerable disincentive for PISPs seeking to enter the market – thus harming competition in the sector. As such, the MLR requirements on AISPs/PISPs should be adjusted accordingly to support the spirit of Open Banking.

However, other members, whilst acknowledging the points on risks, note that at the same time there is a transfer of much of the responsibility for managing aggregate risk that needs consideration of how to address that.

There is a shift from a sector with a developed and mature understanding of financial crime risk – that can now no longer see much of the detail of the underlying transaction, or the networks involved – to an emerging sector that collectively does not yet have a sophisticated understanding of how to manage either the risks in relation to either individual transactions, or on an aggregate basis (in terms of systems being exploited) to spot networks.

This is not a criticism or even a suggestion that individual AISPs/PISPs cannot manage risk – more a recognition that the level of risk management maturity cannot yet be as developed. Therefore, as well as any rebalancing of requirements, this needs to be kept under review by HMG as part of wider consideration of what tools, powers and engagement by public-private partnerships are needed to support a system-wide view of aggregate risk.

Equally, whilst members note the growing fraud risks associated with AISPs/PISPs, the general view is that these can be countered by anti-fraud measures rather than by a need to impose CDD obligations. The bigger issue, outside of the scope of this consultation, but which will need HMT and regulators to take a view, is where liability sits.

For both the issues above, some members suggest that the general stance in the MLRs should be pro-growth, given the low risks of ML/TF, and so requirements be nuanced to reflect the different levels of risk depending on relationship and business model. For example, to ensure that the regime applies but does not require CDD or full CDD to be carried out by PISPs/similar Open Banking services on payment service users.

Most members believe this calibration strikes the right balance on supporting entry whilst ensuring the right framework to manage risks. However, HMG will also wish to consider outside of this SI, the right collective stance on managing fraud risks and how to support industry anti-fraud measures.

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

We note that most PISPs contract with merchants rather than payment users, and that their interaction with payment users will typically not have the element of duration required for a

business relationship. While PISPs will conduct some form of due diligence on merchants, the data retention restrictions imposed on PISPs by the UK regulatory regime makes it difficult for them to conduct CDD on individual payment users. We also note that the Payment Services Directive 2 (PSD2) exempts AISPs from supplying AML/CFT information as part of their authorisation application (Arts 33(1) and 5(1(k))).

We note that the European Banking Authority (EBA) has acknowledged these challenges, and issued sector-specific AML/CFT guidelines for AISPs/PISPs, stating that simplified due diligence will be appropriate in most circumstances. However, we note once again the potential for fraud risk across these products, and the impact that this can have on customers.

We consider that the impact of any such obligations on competitiveness of the AISP/PISP sector, from a commercial perspective, would partly depend on international comparators. We note that the US is currently developing its regulatory framework for account information aggregators, a comparator to AISPs, and does not currently propose to introduce a comparator to PISPs. We also note that the EBA and European Commission have stated that both AISPs and PISPs are obliged entities under the EU AML regime.

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

Members have mixed views on this question. Some believe AISPs should be exempt, but PISPs should remain in scope.

Others believe both should be regulated to manage risk, including fraud risks, and to reduce the risk of unscrupulous companies setting themselves up as AISP/PISPs.

On balance, we recommend that a targeted approach is adopted. There is broad consensus that PISPs reduce the effectiveness of bank's customer monitoring, and that PISPs could help reduce the risk they bring into the system by compensating monitoring of their own (e.g. to identify abnormal volume/velocity patterns, or linked transactions above the E1000 threshold for an occasional transaction). However, further work is required to understand how such PISP monitoring could be implemented within the UK regulatory regime, and how AML regulation could be implemented proportionately to avoid disruptive and low-value activity.

The proposals here link to the points made within our response to the CfE, around distinguishing scope by activity. Not all products /services offered within the financial services sector present ML/TF risk. In the same way as proposed for AISP/PISPs, wider low risk activities within the regulated sector could also be considered to be exempt from the regulated sector. For example, PISPs facilitating cross-border payments will pose a higher ML/TF risk than those only facilitating domestic payments.

Other members note that there are valuable opportunities to consider here, in terms of understanding risk and enriching the intelligence picture, such as when a customer connects payment accounts held in the name of multiple persons in more than one jurisdiction. HMG will wish to consider the most appropriate manner in which to draw upon this information.

In addition, as noted in our CfE response, we believe a principles-based approach should be considered where, rather than on an ad-hoc basis, particular sectors - or services offered by particular sectors - are assessed based on the AML/CTF risk they bring into the system.

Bill payment service providers and Telecoms, 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.**

Our members have mixed views on whether to descope TDITPSPs due to the limited ML/TF risk present, or instead target the legal/regulatory regime to focus on the threats posed by these sectors.

However, for BPSPs it seems there would be no detriment to these remaining in scope. The rationale provided in the consultation notes is that it is highly unlikely that any business in the UK operates as a BPSP. If these entities do not exist, there is no impact upon them through inclusion within the scope of the MLRs. Inclusion therefore allows, if entities did emerge in the future, for BPSPs and any risks they present to be covered. As a result, we think it is best that these are left within scope of the MLRs.

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?**

Our members have mixed views on whether descoping these payment service providers would have any material impact on financial institutions.

There is a potential risk that genuine bills are funded by ML cash, with the payer rewarded in a different method, but some members believe this is a lower risk concern.

Other members believe that the evolving diversity of new payment services makes it more difficult for financial institutions to monitor transactions and to protect their customers from fraud and scams.

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 is hard to envisage a situation when removing an obligation would not reduce the cost and administrative burden of complying with and overseeing that obligation. However, in this case we would question whether the reduction in transparency is justified by the potential savings. Considering the small number of BPSPs and TDITPSPs quoted within the consultation, it seems unlikely that descoping these would have much impact on the cost or administrative burden on either HMRC or registered businesses.

In addition, having a form of public registration of these providers would provide an additional source of information for other regulated firms. This may support their access to payment account services.

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

We do not believe that there would be significant wider impacts here, but would refer to the points we made under Q2 about the right balance between supporting growth and removing requirements in low-risk areas, whilst also preventing exploitation of services and products.

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.

We believe the ML risk associated with individual artists selling their works for over EUR 10,000 is low, especially considering the low number of artists in this situation. We also note that in most instances, there is usually an agency or dealer involved in sales, and it is rare that this would happen directly.

Generally, members view that an artist currently falls into the AMP definition as a "Business trading in" the industry. If the art is sold directly to the purchaser, that would decrease the financial crime risk due to non-concealment of the beneficial owner(s) and final destination of the artwork in question. Key risks in this market include the wide-ranging values involved, the size of the market and the international nature of the market which make it attractive for ML (noting that ML risk was rated as 'high', and the TF risk rated as 'low', within the UK NRA 2020).

A RBA to this could, therefore, involve only including artists that meet the definition of a high value dealer, and exempting the rest. Alternatively, we would welcome a clear definition of “direct sales of art” to provide clarity here.

In addition, the economic crime risk will still remain with the purchaser. Individual artists could still sell their artwork to someone who is trying to conceal their illicit funds. There could be some displacement of economic crime activity from trying to use auction houses/agents etc., whereby money launderers will start approaching lesser-known artists directly, and offering them inflated prices for their artwork (above the real value of the artwork), just so they can “clean” their funds. Therefore, we need to be mindful of making amendments that criminals will exploit, thereby creating a new typology, where the risk is increased by fluctuating values.

As an example, a potential ML typology would be for an “artist” to “sell” dozens of pieces a year just under the Euro threshold. While linked transactions are caught within the scope of the amended Annex D, such individuals are unlikely to voluntarily declare themselves as regulated. In this scenario, HMRC should play a role in detecting such typologies through tax payments by artists (although chances are that money launderers would also not pay tax), and similarly, banks should be prepared to monitor for this typology if emerged. As set out in our CfE response, this highlights the importance of a full system response, rather than the onus being on banks alone to detect new typologies.

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?**

Considering the small number of artists selling their work above the EUR 10,000 threshold, we do not believe this would have a significant impact on HMRC with regards to cost of their supervision.

As per our comments within the CfE response, we note the links between this question and the focus on supervisory effectiveness. We do not think that changes of such a small nature will be able to affect change to the extent that is required, with regards to reducing costs or increasing focus impacting the supervision of this population.

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.**

We are supportive of the proposed drafting amendments in Annex D as adequately covering the exclusion 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?**

Whilst we are not yet sure of the potential here, we do believe digital art is an avenue that could be opened up and exploited by criminals. Digital art would have a clear 'audit trail', and would be less vulnerable to having its value inflated or ownership concealed. However, due to the significant values associated with certain pieces of digital art/non-fungible tokens (NFTs), such assets may soon become a prime target for criminals seeking new avenues to launder the proceeds of crime. These are easy to mint, for example via the Algorand network, with the price assigned by the creator. The same ML risks apply in respect of physical and digital art, therefore the UK legislative framework should include digital art/NFTs within scope of the AMP definition to ensure adequate controls are applied.

We also note the links to use of potentially higher risk products such as non-fungible tokens, where it is easier for artists to gain international exposure than through traditional selling points.

NFTs are likely to be purchased using cryptoasset tokens. Whilst there are some mitigating controls when ownership is stored on a publicly available register, some ownership can be anonymous. With the cryptoasset industry being brought into scope of the MLRs, it seems fitting to extend the AMP definition to include trading in NFTs and possibly other areas of digital art. There still needs to be consideration given to Source of Funds, which is an industry challenge due to potential purchase with crypto and any third-party involvement in transactions. We reiterate our comments on fluctuating values and emerging typologies here, as noted under Q9. We also note the relevance of the cryptoasset travel rule to NFTs, as noted under Q58 below.

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 do not believe that the provision of individual SAR information by reporters would necessarily allow enhanced performance of supervisory functions, not least as it is difficult to see how supervisors would be a more effective assessor on what makes a good or acceptable SAR than the NCA itself.

Supervisors need to know the risks for their sector as a whole, and for this reason are likely to be more interested in the topics and targets of the SARs collectively, rather than looking at individual SARs. Access to SARs (direct access preferably as per answer to Q17 below) may have a role to play in a data-led approach to supervision, provided that supervisors do not provide subjective rulings on whether individual SARs meet the criteria under the Proceeds of Crime Act (POCA).

Equally, this needs to also reflect the challenges still present in levelling up of standards and understanding of supervised populations across our supervisors. There would be an unevenness across supervisors in relation to how this power was used and for what purpose.

It is difficult to see how this power would actually drive-up standards in the financial sector, and could in fact lead to more defensive reporting, not for the purposes of suspicion per se, but due to concerns over supervisory expectations.

We also believe there is limited utility as many of the financial sector SARs will be in relation to activity in a sector where there is a separate supervisor to the FCA. It is difficult to see, for example, how a bank sharing a SAR with the FCA on a property transaction involving the legal and estate agent sector, strengthens the overall regime – or indeed the effectiveness within an individual firm. Equally this would run the risk of increasing resource on low utility activity, in terms of a firm providing a SAR that the regulator could receive from the NCA if there was an issue.

We believe the same impact could be achieved by encouraging more direct sharing between supervisors and the NCA, particularly where the NCA has concerns over the SARs received. Obtaining access directly from the NCA, rather than creating a new process whereby supervisors can request SARs from FIs, would be the option that would have the least operational impact.

Members believe there is merit to a more structured approach to feedback, both between the NCA and supervisors, and also between the NCA and reporters. Greater granularity of sectoral and individual feedback could help raise standards across the ecosystem. We believe this requirement may therefore fit better under the NECC governance structure.

However, industry is strongly committed to their ongoing efforts to bring about positive changes within the existing SARs regime. If supervisors believe this would be useful intelligence to support their efforts in tackling financial crime, and steering the development of a RBA to supervision, then we are supportive, so long as there are clear parameters introduced. If, however, it is the supervisors' intent to acquire SARs in order to assess the quality and appropriateness of the quantity of SARs submitted by supervised entities, we would argue that such a quality assessment is already being performed by the NCA/FIU who have recruited additional staff as part of the Economic Crime Reform Programme precisely to support this functionality and associated outreach to reporters.

The AML/CTF regime relies on a significant amount of processing (sharing/analysing etc.) of personal data in order for it to function. Therefore, the absence of a mention of the interaction between the regime and the requirements of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) is noted. Understanding the interplay of the two sets of requirements (GDPR and MLRs) is key to ensuring necessary and proportionate application of the MLRs, to ensure we combat financial crime in a fair, transparent and accountable way. The MLRs neither specifically refer to the GDPR, nor contain any information on how the GDPR's boundaries (e.g. allowing the processing of data for crime prevention and detection purposes) interact with Reg 52 powers under the MLRs. This situation should be clarified at the same time as considering amending and indeed broadening the scope of Reg 52, preferably in tandem with the Information Commissioner's Office (ICO). On that basis, we suggest that this consultation should involve significant input from the ICO and DCMS. We need clear guidance on how to navigate between the two regimes, and would welcome clarity on the retention schedules set out in the current MLRs - they are extremely difficult to understand and implement.

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?

We believe it could be argued that the current text contained within Regulation 66 is sufficient to allow supervisors to access the contents of SARs, through the inclusion of the permission for a supervisor to require a relevant person to provide specified information or documents, or information/documents of a specified description. If a SAR is considered to be a 'specific document or information', it would allow for such documents to be requested by a supervisory authority.

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?

There are a number of fundamental considerations here that we do not believe have been addressed by the consultation.

There needs to be further clarity on how the FCA intend to use the data received in SARs. We also note that receiving individual SARs on request from their supervised population may only provide limited intelligence as one piece of a potentially large puzzle.

As per our answer to Question 13, if the purpose of increased access to the content of SARs is for supervisors to assess the quality of SARs, this would seem to run contrary to the role of the FIU and National Economic Crime Centre (NECC), which brings together parts of the public sector, including the FCA, to drive and coordinate activity and improvement across the system.

Given the FIU is hosted in the NECC, it would seem more appropriate for the NECC to decide where it wishes to flag systematic and individual issues with regulators, as it is the FIU and the NECC who have a more holistic view of good and poor SAR reporting on an individual and thematic basis.

We would also request further clarity on how the data contained within SARs intends to be stored and protected within the FCA/supervisor systems.

We note that the CfE is exploring the existing capabilities of AML supervisors, and believe further consideration needs to be given to the impact the addition of these responsibilities would have on the capabilities of supervisors across the regime.

Any agreement for access to SAR content must be in conjunction and agreed with the ICO to ensure GDPR concerns are considered.

16. **Do you agree with the proposed approach of introducing an explicit legal power 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 (in the event a view is taken that a power doesn't currently exist)?**

We encourage the introduction of clear drafting within the MLRs, so support the introduction of clarificatory language if required.

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.**

This is dependent on the specifics within which this requirement is introduced.

It could be significant if it adds another layer of reporting requirement to regulators (outside of regulatory visits or industry requests for information) with little clarity on what benefits such a report would drive. The impacts would also be let more significantly by a high reporting sector compared to a sector where reporting is flagged as low.

We believe it would be best if the requirement is introduced with no additional administrative burden to the private sector, e.g. the FCA is granted access to the current SAR reporting system at the NCA, rather than generating additional reporting obligations 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**

might be put in place to address these? Please provide suggestions of potential mitigations if applicable.

It depends on the purpose. The FCA, or indeed other supervisors, are not in a position to assess whether a SAR is high quality or high value to law enforcement. SARs can only 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.

If the FCA were to be given access to SARs, we would expect the FCA to also take on a greater role in issuing guidance over when SARs should and should not be reported. Whilst we understand that the FCA is opposed to such an approach, it would seem a logical progression of their role of viewing the content of the SARs from their supervised population to reach a view and support both effective reporting and upholding a RBA.

We fail to see how they could not reach a view on such issues, and as such it would seem appropriate for them to ensure their view is understood by the industry in order to support effective financial crime risk management.

We believe there is value in this, if supervisors intend to use information contained within SARs to help their supervised populations to improve their systems and increase effectiveness. Where it would not be helpful is if these powers were to be used to support enforcement investigations, as we do not believe this would be a legitimate purpose, and, as noted above, believe there are limitations to the value in being able to see individual SARs.

We believe there needs to be the correct technological capabilities in place to allow supervisors to store and manage SAR data appropriately as well as the sufficient capability and understanding of what constitutes a 'good' SAR.

As per NCA reporting, there are mixed levels of SAR submission across the breadth of sectors subject to the MLRs. Unrestricted access to SARs by supervisors could result in the unintended consequences of certain relevant persons becoming more reluctant to submit SARs if this may expose any systems or controls weaknesses, which could result in subsequent regulatory scrutiny/enforcement measures. Inclusion of this requirement could, therefore, serve to exacerbate this issue.

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?

We are supportive of the requirements 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.

Where the definition of a 'financial institution' is not explicit, this may result in a relevant person considering a wider scope of customers as falling within the definition of a 'financial institution' and as such, the obligation to treat such relationships as 'correspondent relationships' as defined by Regulation 34(4) which includes "the relationship between and among credit institutions and financial institutions". Updating the activities that make a relevant person a financial institution may help to narrow this broad definition, that currently encompasses non-bank financial institutions

Greater alignment to FSMA would also be welcomed, in order to align with activities set out under the Regulated Activities Order 2001.

There is divergence in the EU on regulatory definitions – one example is the EU definition of a "credit institution". This solely relates to deposit takers under the EU Capital Requirements Regulation (CRR), which conflicts with the EU's CRD IV definition, which includes investment banks and some asset managers. Whilst this was corrected under UK law under the EU Withdrawal Act 2018, it makes sense to align to UK requirements to preclude confusion.

One notable gap is lending for Commercial customers, which is not regulated in the UK unless it involves specific financial instruments, such as derivatives – whilst lending is regulated for consumer credit and home finance activity. Whilst most large institutions will be captured, perhaps this anomaly could be added to the MLRs to capture smaller firms who may not perform a wide range of activities.

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

Yes, this would be beneficial for smaller firms – larger institutions are licenced for many activities. It would provide comfort for larger institutions in order to offer banking services to a wider group.

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

As set out in our response to the CfE, there are certain sectors that bring risk into the system, both fraud and ML risk, that should be brought into scope of the MLRs. This includes some unregulated small legal and accountancy firms, as well as social media and telecoms companies for example.

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.**

It would likely be a benefit to larger firms, as noted under Question 20. The sectors who may potentially be affected would be best placed to comment on direct costs and any operational/resourcing impacts.

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.**

If the FCA's remit is expanded, this could impact on their supervisory effectiveness.

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?**

We do not believe there will be significant unintended consequences here.

As set out above, there is divergence in the EU on regulatory definitions – one example is the EU definition of a "credit institution". This solely relates to deposit takers under the EU Capital Requirements Regulation (CRR), which conflicts with the EU's CRD IV definition, which includes investment banks and some asset managers. Whilst this was corrected under UK law under the EU Withdrawal Act 2018, it makes sense to align to UK requirements to preclude confusion.

Aligning should theoretically support firms in fully understanding their obligations by providing further clarity, as well as supporting internal processes.

Proliferation Financing Risk Assessment

We support UK reform to implement the October 2020 amendments to FATF Recommendation 1 (i.e. requiring countries, financial institutions and Designated Non-Financial Businesses and Professions/DNFBPs to identify, assess and mitigate the risk of potential breaches, non-implementation or breaches of the targeted financial sanctions related to proliferation financing (PF) as set out in FATF Recommendation 7). We also welcome the UK's National Risk Assessment for Proliferation Financing (PF-NRA) and its acknowledgement that UK PF risks arise from a range of sectors, including finance, maritime insurance, DNFBPs, manufacturers of military and dual-use goods, and academic research.

However, the overwhelming majority of members consider that the proposed amendments to AML/CFT obligations on the regulated private sector are a disproportionate interpretation of these amended FATF requirements. As noted by the consultation (para 4.8), FATF Recommendation 1 refer "strictly and only to" targeted financial sanctions under United Nations Security Council (UNSC) resolutions relating to the proliferation of weapons of mass destruction and its financing (i.e. UNSC regimes for Iran and North Korea). In contrast, the proposed amendments could be interpreted as requiring firms to conduct a standalone entity-level risk assessment of PF and assess their exposure to PF risk beyond the potential breach, non-implementation or evasion of targeted financial sanctions for Iran and North Korea (or PF risk as defined by FATF).

We would welcome clarity on this as most members consider that such a standalone requirement is not necessary for implementing FATF requirements, and that relevant regulated private sectors should be able to consider PF within the scope of existing risk assessments, in line with the FATF's proposed approach. We would also suggest aligning the proposed changes to the MLRs with the approach for the PF-NRA, which explicitly allows HMT to consider PF within the scope of the existing national AML/CTF risk assessment.

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

The overwhelming majority of our members do not agree with the proposed definition. As noted above, the proposed definition goes beyond PF Risk and would therefore result in a disproportionate interpretation of the amended FATF Recommendation 1.

The proposed FATF definition that has been included in the MLRs is much broader than PF Risk and open to interpretation, even though it is limited in application to the DPRK and Iran regimes. It will require some clarification in terms of operationalisation, particularly on the possibility of screening goods which is not common practice. If the purpose of the amendments to the MLRs to align with FATF Recommendation 1 changes, then this definition will need to be narrowed.

If the expectation is for firms to have an understanding of broader PF risks, as defined by the FATF, then this will need to be clarified and appropriate guidance provided.

The adoption of a broad definition will also present challenges in terms of identifying such activity. A more manageable approach would be if the expectation is on the basis of reasonable measures being taken to identify such instances, or where government authorities have provided information to identify such activity.

Some members believe if the narrower definition of PF Risk is adopted, it is not appropriate for this obligation to form part of AML/CTF obligations (i.e., the MLRs). Instead, they believe that it would be preferable to instead adopt a similar approach as applies to sanctions risk assessments, for example, by applying the new requirement via regulatory guidance. Alternatively, if a legislative change is the preferred approach, we would suggest integrating the proposed PF-NRA and PF

policies, procedures, and controls requirements into Regulation 18 and 19 rather than as a standalone provision, incorporating an exemption for obliged entities that are out of scope of these requirements.

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.

We agree that PF should be considered as part of the MLRs, but consider that this should be within the scope of existing risk assessments. We believe the drafting of this chapter would result in a disproportionate interpretation of FATF requirements and does not reflect actual PF threats.

As above, the large majority of members believe that requiring the consideration of PF as a standalone risk assessment would lead to duplication in effort, be disproportionately burdensome on resources, and have limited impact on ML/TF. This amendment would pose particularly challenging for smaller firms, or those not closely aligned to the FATF definition of “proliferation financing” referenced under Q25 above.

We believe that considering PF as part of existing AML and sanctions programmes would be sufficient to meet the expectations set out by FATF.

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

PF is generally currently considered as part of existing sanctions and ML/TF risk assessments; i.e. not as a standalone risk assessment.

For example, PF may be a relevant factor for customer risk assessments where relevant, based on the nature of the firm, where it operates, its customer base, and the products and services it provides. In addition, such PF assessments are of particular interest in respect of Trade Finance products and dual use goods.

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.

This could be addressed through existing CDD measures, so the impact would be minimal. However, for some firms addressing clients involved in the manufacture/sale of strategically controlled goods, the proposed requirement would require additional resource, particularly in the identification of the clients that would fall into such a category (either completed internally by asking all clients if they deal in such goods or externally through the provision of lists of such entities enabling a more targeted approach).

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?

We believe that no new powers should be required, as PF risks, as defined under the recent changes to FATF Recommendation 1 to be largely handled through existing sanctions controls. As a result, we expect the role to be more of an oversight role and the provision of guidance on assessing PF risks, potential PF red flags, and regulatory expectations in terms of PF policies, procedures, and controls.

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.
The majority of requirements in the proposed drafting will already generally have been addressed through existing sanctions compliance programmes, as appropriate to the nature and size of a firm.

Once again, we believe that rather than establishing separate controls and procedures – which would lead to duplication in effort and increase the burden of resources required – it would be more effective to adapt existing sanctions and AML/CTF sanctions programmes to include PF, where possible and as appropriate to the nature and size of a firm. Indeed, some members have confirmed that this is the current approach, implemented subsequent to the amendments being made to FATF Recommendation 1.

Extension of the terms 'Trust or Company Service Provider' and 'business relationship'.

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?

Trust & Company Service Providers (TCSPs) present well known and longstanding vulnerabilities within the regulated sector. This is emphasised in the National Risk Assessment 2020 which increased the TCSP risk score for ML from medium to high, and in the dedicated Public-Private Threat Update issued under the Economic Crime Plan 2019-2022 on TCSPs.

Slightly separately, issues in supervising TCSPs, who already form part of the regulatory regime, have also recently been underlined by the OPBAS Report 2021, which noted that many Professional Body Supervisors have still not effectively prioritised their AML supervisory work. Due to the associated risks of TCSPs, which are the highest risk services provided by Alternative Service Providers for ML purposes, we would welcome this proposed change along with parallel focus on continuing to improve the supervision of TCSPs who fall within the existing scope of TCSPs and any subsequent expansion in scope.

Clarifying the scope of AML/CFT regulated services and business relationships will support consistent TCSP approaches to CDD. This would greatly support the Government's Strategic Priority Six (Transparency of Ownership) under the Economic Crime Plan, including CH reform proposals for verification of Limited Partnerships and reliance on the CDD of UK supervised TCSPs.

This Economic Crime Plan Priority also includes UK efforts to promote stronger international action on ownership transparency, such as potential updates to FATF Recommendation 24 (the transparency and BO of legal persons), which is currently under public consultation.

We agree that the regulations should be expanded to cover the formation of all forms of business arrangement, including LPs registered in England and Wales or Northern Ireland.

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

The current definition in Regulation 4 of the MLRs of a "business relationship" highlights the commencement of a business relationship as the time when a contract is established, that also includes an element of duration.

We believe that the term "business relationship" has a broader meaning than set out in this definition, which is not flexible enough to include other scenarios, where contracts are signed for

specific products (e.g. ISDA, lending, cash accounts) but not necessarily for all products. There may be instances, for example, for FX products, where there is no written contract with a customer, but there is a business relationship.

We believe that the definition of "business relationship" should be revisited to include other possible scenarios, where there may not be a written contract with an element of duration. We would appreciate clarity and examples on the definition of business relationship, and would recommend adding syndicated lending and brokerage services to the examples listed. We believe clarity is needed in this area to avoid unintended consequences that increase the cost of compliance for ultimately lower risk business relationships and in turn, possibly make them commercially unattractive for our members to engage with.

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 to this question.

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 to this question.

Extension of the terms "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 CH. We consider that clarifying the scope of business relationships in this manner will support more consistent TCSP approaches to CDD and integrate TCSP practices with the intended aims of CH reform.

Company formation and associated TCSP services continue to be the highest risk services provided by Alternative Service Providers for ML. As noted within the UK NRA 2020 and SRA Thematic Review from 2018, these can enable the laundering of millions of pounds, conceal the ownership of criminal assets and facilitate the movement of money to secrecy jurisdictions. Many are offshore and pose a significant risk, particularly when they act as nominee shareholders and/or there are other associated High or Higher Risk factors.

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)?

We agree that Regulation 4(2) should be amended to include a relationship where a TCSP is acting or arranging for another person to act as those listed in Regulation 12(2)(b) and (d).

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

We agree that the one-off appointment of a limited partner should not constitute a business relationship considering they have no management role.

However, we would welcome more details regarding how this would work in practice. On the one hand, allowing the limited partner to be added to CH records regardless would allow firms to assess the associated FC risk. On the other hand, if one-off appointments do not constitute business relationships, then they may not be subject to TCSP CDD (e.g., if also falling under the threshold for an occasional transaction), which would have an impact on CH reform.

There could be the unintended consequences for unscrupulous parties to add and remove partners individually in order to preclude CDD requirements under the MLRs, whilst these parties could still inject funds into the LP. Therefore, further background on the practical impact of this requirement would be appreciated.

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

Whilst we cannot comment on the impacts on TCSPs themselves, there may be operational impacts for banks if CDD had already been conducted and a RBA applied to the relationship, resulting in the requirement for remediation exercises.

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 to this question.

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.

As per our response above, there may be operational impacts for banks if CDD had already been conducted and a risk-based approach applied to the relationship, resulting in the requirement for remediation exercises.

Reporting of discrepancies: Expansion of Regulation 30A to introduce an ongoing requirement to report discrepancies in beneficial ownership information.

We welcome the objective in the separate CfE consultation of preventing the abuse of UK corporate vehicles, and strongly support ambitious CH reform. However, we question whether discrepancy reporting obligations have proven effective in preventing abuse, and remain unconvinced that results to date justify the significant private sector resource required and the potential for additional delays and customer friction.

As a general comment, we are surprised that this proposal does not reference the overlapping CH reform proposal to extend the scope of discrepancy reporting to include directors and registered office addresses, and the additional CH reform proposals for scrutiny of company registration. As noted above at Q31 et al, this consultation and the CfE include a number of proposals that directly impact on CH reform. We consider that these related proposals should be developed holistically, to ensure proper targeting, proportionality and coherency of the overall obligations on the regulated sector. This should include proper consideration of whether reform of obligations on UK bodies corporate under MLRs Reg 54 and the corresponding Companies Act obligations could prove more effective in preventing and deterring abuse, e.g. by requiring companies to file proof of identity for their beneficial owners and directors.

Equally, we consider that UK reforms should take account of international developments, including the outcomes of the June 2021 FATF consultation on Recommendation 24. Clearer definition of key FATF requirements and a programme to support consistent national implementation would not

eliminate all abuses, but would reduce the complexity and blind spots of the current international system.

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.

Registration of beneficial owners of companies and legal entities is a crucial gateway for transparency of ownership and a key tool in the prevention of financial crime. We believe that sufficient resourcing of CH, coupled with effective sanctions on companies who register incomplete and misleading information, is the most effective way to prevent misuse of the system and transparency of ownership.

As noted above, we question whether discrepancy reporting has proved effective in preventing abuse of UK corporate vehicles and consider that a more holistic approach is required, including alignment with wider Company House reform and review of AML/CFT effectiveness. Within the context of a more holistic approach, while we are strongly supportive of CH reform, it is not clear whether this proposal will form part of a more effective whole-system response to economic crime. Additional private sector checks can support a more effective approach to the overall AML/CFT regime, but only where matched by adequate public sector resourcing, information sharing and focus on high-value activity.

Any extension to the current discrepancy reporting requirements should be proportionate and based on sufficient empirical evidence of its effectiveness in combating economic crime. We are not aware of a clear evidence base for the effectiveness of the current discrepancy reporting regime, such as increased CH enforcement or amendments to the PSC register to resolve confirmed material discrepancies. We are also not aware of a comparative cost-benefit analysis of the proposed extension in obligations on the regulatory sector vs. public sector methods of reducing discrepancies, such as verification, information sharing and cross-checks on CH data.

This compares to significant private sector resource required to implement this requirement, including assessing whether identified discrepancies are material or not, which could have been allocated on alternative AML/CFT activity. We consider that this opportunity cost would be multiplied many times over if discrepancy reporting obligations were extended to ongoing CDD, and again if separate CH reform proposals were implemented to extend the scope to directors.

We reiterate once again that it is not the responsibility of the private sector to ensure the data held at CH is accurate and robust. We believe that the only truly effective approach here is to introduce verification capabilities within CH, through existing reform efforts, as well as controls to review accuracy of their own data on an ongoing basis. This would align to FATF recommendations. The responsibility for oversight and accurate BO should sit with the companies registering with CH, and CH as the owner of the PSC register.

We are aware that currently, CH resource is stretched, and faces challenges keeping pace with the number of discrepancies reported. This results in discrepancy reports being picked up several months after the report was made, by which time the report is often no longer relevant, customer data has changed again, and we are only able to assist with historical customer details.

Further, we are of the view that it is the registered entities themselves that should be under clear and enforceable obligations to keep their data on the CH register accurate and up to date. We are unsure of the extent to which legal entities currently observe such obligations, or indeed are aware of the tangential obligation contained within Regulation 43 of the MLRs to inform their bank within 14 days of a change in ownership (or other due diligence) data. At the moment, there is no deterrent for companies, and this feedback formed part of the industry's response to FATF's review of

Recommendation 24 (Beneficial Ownership). The Government should be investing in resource and sufficient engagement between CH and HMRC, who monitor the companies registered for tax compliance.

We consider that the proposals for an expansion in discrepancy reporting and the wider CH reform package need to be developed holistically. We consider that data quality problems in CH are best addressed by public sector verification of company filings and ongoing monitoring of registry data. We also consider that ongoing monitoring would be supporting proposed enhancements to public sector information sharing by and with CH, and that in many cases public sector information sharing would provide the most efficient and effective method of identifying and evaluating discrepancies in registry information.

Additionally, if discrepancy reporting is pursued as part of a more effective approach to AML/CFT, then this requires corresponding amendments to other obligations on regulated firms. We consider that CH reform should allow bulk reporting and provide timely and specific feedback to firms reporting discrepancies. We also consider that MLRs Reg 28(9) should be amended to allow firms to rely solely on CH data to identify and verify BO of their UK corporate customers.

Further clarity is also required around the extra-territorial application of any discrepancy reporting obligation for UK firms with branches and subsidiary undertakings outside of the UK. For example, clarity on whether beneficial ownership (BO) discrepancies are reportable for all UK corporation even if the business relationship is not within the UK, e.g. UK corporation onboarded in Hong Kong.

There remains a misalignment between the definition of Beneficial Owner under the MLRs and People with Significant Control (PSCs), and the registration requirements for PSCs which may include legal entities and not a natural person/individual. The Government needs to address these issues before expanding the current obligations.

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

We believe that the obligation to report a discrepancy when a regulated firm 'should reasonably have become aware of', as stated in Q.42, is fairly broad and open to interpretation. Introducing this term is not helpful, as regulated firms already have an obligation under Regulation 28(11)(b) to keep information and documentation up to date. We recommend wording similar to when conducting CDD measures under MLRs reg 27.1 and 28.11.

The consultation refers to 'any' discrepancy. The legislation needs to make clear that it refers to reporting material changes to the BO, rather than 'any' discrepancy. These issues will lead to an increase in overreporting and significant additional cost to relevant persons.

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

We reiterate once again that it is not the responsibility of the private sector to ensure the data held at CH is accurate and robust. CH does not require companies to be registered by UK regulated company formation agents or to have an established business relationship with another UK regulated sector firm, and case studies of the so-called Laundromats and other abuses of UK corporate structures have noted that many of these structures did not involve the UK regulated sector. We believe the only truly effective approach here is to introduce verification capabilities within CH, through existing reform efforts, as well as controls to review accuracy of their own data on an ongoing basis (e.g. using volume/velocity checks to help identify potential problems at an early stage) with support from new powers for public sector information sharing and data matching. This would align to FATF recommendations.

Alongside verification, CH could also conduct a review (including any re-verification needed) of PSC information with the registered entity within a set timeframe (e.g. annually/bi-annually). This would provide relevant persons with comfort in terms of the information on the register, alongside introducing a more beneficial use of CH resource, as opposed to dealing with backlogs of potentially outdated information.

We reiterate the point made above that there should be more of a focus on the identification and enforcement of sanctions against companies registering incomplete and misleading information. At the moment, there is no deterrent and this feedback formed part of the industry's response to FATF's review of Recommendation 24 (Beneficial Ownership).

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?

We believe that this change, adopted piecemeal and without alignment to a more holistic approach including wider CH reform and a more effective AML/CFT regime, provides minimal benefits to the prevention of abuse of UK corporate bodies, with significant cost on the relevant persons, as per our answers to the previous questions.

We consider that a full cost benefit analysis is required to support review of current requirements and the proposed extensions. As noted above, we are not aware of a clear evidence base for the effectiveness of the current discrepancy reporting regime, such as increased CH enforcement or amendments to the PSC register to resolve confirmed material discrepancies. We are also not aware of a comparative cost-benefit analysis of the proposed extension in obligations on the regulatory sector vs public sector methods of reducing discrepancies, such as verification, information sharing and cross-checks on CH data.

Chapter 5: Information sharing and gathering

We note that Regulation 52(c) still refers to 4MLD when defining an overseas authority.

Disclosure and Sharing

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

We agree with the proposal that the Regulation 52 gateway under the MLRs should be expanded to allow for reciprocal protected sharing from relevant authorities (including law enforcement) to supervisors.

We believe that this should be done in a controlled manner, with an appropriate framework surrounding it, to ensure certain thresholds still have to be met to access information.

Some members believe this should be introduced purely for the purpose of assisting law enforcement agencies with investigations, and data sharing must be limited to information that is necessary for such investigations.

It would be appropriate to gain clarification on what BEIS would use such intelligence and information for, before expanding the scope of Regulation 52. As set out above, in an effort to continue strengthening the quality of information held on CH, we see value in BEIS using this information to analyse CH data in order to identify anomalies and typologies.

We note that BEIS' Insolvency Service Criminal Investigations Team are increasing their focus on Economic Crime and Fraud, using their powers to prosecute specific offences under insolvency and company law (including insolvency-related fraud, for both individual and corporate defendants). Offences include fraudulent trading, acting as a company director whilst disqualified, destroying company records etc. In the period 2019 – 2020, the Insolvency Service initiated 142 criminal prosecutions, with a further 143 live investigations in the pipeline. These cases can include breaches of the MLRs. This activity demonstrates that BEIS could prove to be an effective AML/CTF supervisor. As ever, sufficient resourcing and clear mandate on powers must be available for any relevant authority to effectively carry out their obligated duties.

If BEIS were to be added, we would not expect this to create a de facto reporting requirement where BEIS wanted to gather further information in a way that would not be pursuant under existing gateways and mechanisms.

Equally, if BEIS were to be added, we would expect them to in turn share information and intelligence with the regulated sector to tackle systematic issues and vulnerabilities, such as emerging risks in relation to company formation at CH. The use of mechanisms, such as the Joint Money Laundering Intelligence Taskforce, would seem suitable for such an approach. Improved information sharing amongst government agencies could have benefits for improving the quality of data held by CH.

The final area we would point to is that BEIS and in turn CH cannot always act on the information and intelligence it currently receives – such as in relation to discrepancy reporting where a company on which a discrepancy has been reported can refute that and CH has no real power to compel a change. Closing this resourcing and capability gap would seem a more pressing need than adding BEIS to the relevant authorities for the purposes of Regulation 52.

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

The intelligence and information sharing gateway provided by Regulation 52 may be beneficial in allowing firms to go direct to a law enforcement agency, rather than having to go through the NCA. This would, of course, require clear parameters in place in order to provide reporting clarity and prevent any reporting errors.

We also support this power being extended to mandatory sharing of relevant intelligence and information with banks, as well as much wider cross-border sharing. This would align with the industry ask for a wider set of holistic powers on information and intelligence sharing to allow far more sharing, with protection from civil litigation, between and within the regulated sector.

HMT should also consider how risks come into the sector from non-regulated (for ML purposes) sectors and new and emerging sectors. So, for example, due consideration should be given to whether bodies such as OFCOM and DCMS should be included in the scope of Regulation 52.

There is member support for extending 50(4) to cover any situation where the relevant person or bank operates in the UK, rather than only applying to overseas authorities when the relevant person is headquartered in the UK. This extension of powers would enable a broader range of "authorities" to be engaged in countries where specific threats to the UK originate.

Should any amendments be made to the current SAR reporting process under Regulation 52, whereby firms could report to authorities outside the NCA, this would need to be clearly defined in order to prevent reporting errors. Firms are still subject to the POCA reporting obligation and creating additional reporting channels risks, complicating things for both firms and law enforcement and may

lead to connections between disclosures being 'missed'. A suitable alternative could be that the existing regime remains, and the NCA continues to refer SARs to other agencies for us, noting this may cause an administrative burden for them. HMG should be mindful of the potential penalties that errors could lead to, for both individuals and relevant persons.

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?

We believe that expanding the Regulation 52 gateway to allow greater information sharing amongst authorities should be supported, as long as it is controlled, and shared with other supervisory authorities where needed.

The same point as above in ensuring there is a more holistic consideration of how risks now enter or crystallise in the wider ecosystem applies here and whether a greater range of authorities and supervisors should be in scope consummate with the arguments made in the separate CfE on extending the scope of the MLRs.

Equally, for any additional expansion of the range of public authorities and supervisors that can utilise the Regulation 52 gateway, there should be an expectation that as well as receiving information, they should contribute their analysis of newly acquired information and internal data towards a greater holistic public-private understanding of threats, at a minimum through the generation of typologies. The collective fight against economic crime can only be strengthened by, as appropriate and necessary, increased sharing between and within the public and private sectors by all relevant parties.

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, which is why it is important that information shared by supervisory authorities must be shared on a need-to-know basis, with the firm remaining informed on when this information is being shared.

As per our response to Q13, there also needs to be consideration given to GDPR requirements.

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

The expansion of Regulation 52 may create challenges, including additional cost and administrative requirements on the supervisory authority.

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?

This is not an issue where members have a strong view. However, as made elsewhere, we think a wider look at information sharing powers on economic crime is needed.

Information Gathering

We are sympathetic to the general proposals, but it would be helpful to understand further the reasons why the FCA considers it necessary to be given FSMA-equivalent powers in respect of Annex 1 entities, and why their existing powers are not deemed to be sufficient.

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.

Our starting point is that regulations and supervision should focus on type of activity as opposed to type and size of firm alone and that the supervisor, in this case the FCA, should have the powers it needs to understand and manage risk on that basis.

Equally, any requirements should be proportionate to size, activity and risk and as a general principle, as set out in the CfE, the FCA should have a focus on supporting effectiveness and efficiency in their supervised population, including with regard to regulatory burdens on all firms.

As part of an expansion of powers, we also believe that the FCA should help firms understand and manage risk in relation to relationships within the full population that it manages and supervises or jointly supervises with another public sector supervisor.

So, for example, where one part of the FCA supervised population, such as pawnbroking services, may find it harder to gain access to banking services for reason of commercial risk appetite and concerns over cost of compliance by another part of the FCA supervised population, then the FCA should help manage those concerns and tensions.

Examples of activity that this could encompass includes setting out clear expectations on both parts of their supervised population, and how to demonstrate those expectations have been met. This would include setting out what appropriate risk mitigations would be and how to move toward a more simplified due diligence approach where appropriate.

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.

As a starting point that would seem appropriate, but only if it uses and exercises those powers in an appropriate manner, and uses those powers to help manage risk effectively across the entire ecosystem.

As above, that includes the FCA taking a more active role in helping firms understand and manage risk in relation to business relationships within the full population that the FCA manages and supervises or jointly supervises with another public sector supervisor.

For example, the cryptoasset business has a different risk profile to banks, and arguably a limited control framework in comparison, so we do not feel it is appropriate for their supervision to be aligned to supervision/enforcement in relation to more mature sectors – rather, more intensive effort should be invested in supervising possibly less mature high-risk entities until a degree of maturity is established. If any riskier sectors (such as social media firms) are brought in, they should be calibrated under a robust benchmarking exercise.

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.

It would seem logical, based on the caveats at the start of his section, for the FCA to be able to understand and manage structural and thematic risks more easily.

The effectiveness would come from how the FCA would use those powers, such as supporting access to banking or in a more interventionist approach on tackling cashing out.

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.

If implemented and used correctly, this expansion of powers could lead the FCA to play a greater role in helping understand and manage risk, and mitigation of risk, across the entire population it is responsible for supervising.

However, increasing the FCA's supervisory remit could reduce their effectiveness if this causes them to be overextended, which could potentially dilute their supervisory effectiveness. As a result, any expansion of scope should be based on tangible efforts to disrupt and prevent Economic Crime, ensuring that no undue burden is placed on relevant persons.

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.

There would be a small expansion of resources needed, but this plays back to a principle we articulated in our response to the Levy that those bringing risk into the system should help contribute, so we would expect a corresponding increase in fees for Annex 1 firms to help manage those risk.

On wider impacts if, as suggested, the FCA play a wider role in providing clarity on management and mitigation of risk then there would be a natural evolution in stance, but one that we think would help strengthen the ecosystem.

Cryptoassets: The approach to implementation

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

In general, we welcome the principle of requiring the cryptoasset sector to provide information about the originator and beneficiary of transactions, in line with new FATF standards. Greater transparency would support tracing of cryptoassets and could help deter criminal abuse, such as currently seen through high volumes of cryptoasset investment scams. Consistent regulatory standards and enforcement for the cryptoasset sector could also help to build trust with the banking and finance sector, supporting collaboration in the fight against economic crime and in protecting our mutual customers from fraud.

However, the specific proposals to begin implementation of the "travel rule" for cryptoasset transfers raises concerns across members, as, while in principle we welcome the drive to comply with FATF requirements and mitigate the ML risks associated with cryptoasset transfers, the proposals include divergent approaches from proposed EU requirements, in particular by permitting lower levels of information to accompany intra-UK transfers, and by setting a GBP threshold which will lead to additional complexity as to the applicable payment information requirements given shifting exchange rates.

We also note that, while Singaporean requirements in place since January 2020 also allow for divergent approaches for intra-Singaporean and cross-border transactions, this only applies to information required to be provided immediately and that the full scope of required information must be provided on request for both intra-Singaporean and cross-border transactions.

We believe it is crucial that the approach taken allows for a standardised process across jurisdictions, as divergent regulation is inherently part of the risk profile for cryptoassets. We note the Egmont Group of FIUs' 2018 Typology of Virtual Currencies that reported that national FIUs have identified challenges associated with inconsistency of national regulation. We also note the JMLIT Future Threats Working Group conducted a late 2018 study of scenarios for evolution of threat of criminal abuse of cryptoassets, identifying international regulatory consistency as key drivers for the threat.

The fundamental challenge will be avoiding a disjointed, decentralised approach to what ideally needs to be a standardised process and set of requirements across jurisdictions.

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.

As noted above, greater transparency of cryptoasset transactions could reduce costs on the financial sector by supporting tracing of cryptoassets and thereby helping to deter criminal abuse, including high volumes of cryptoasset investment scams against our members' customers.

Consistent regulatory standards and enforcement for the cryptoasset sector could also help to build trust with the banking and finance sector, supporting collaboration in the fight against economic crime and in protecting our mutual customers from fraud.

The impact of disjointed requirements will be significant. We believe it is crucial that the approach taken allows for a standardised process across jurisdictions, as divergent regulation is inherently part of the risk profile for cryptoassets. However, we would welcome a suitable approach to make sure there is an appropriately nuanced treatment strategy, e.g., taking into account the varied risks and controls between an 'over-the-counter' cryptoasset exchange and a wholesale market customer trading in cryptoasset futures.

Any UK legislative update should provide sufficient flexibility and consideration to developments in global standards and implementation, in an effort to encourage harmonised rules globally.

There is currently no technological solution for global travel rule implementation and any UK legislative update should provide sufficient flexibility and consideration to the developments in the global standards and implementation.

The costs of implementation are difficult to estimate in the absence of interoperable technological solutions, the complexity of cryptoassets and the underlying decentralised ledger technology.

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?

Yes, we believe a grace period is appropriate. We consider that the implementation period should allow active government consideration of global developments and regulatory dialogue to support international harmonisation. We consider that the grace period should be, at a minimum, till the next FATF implementation outreach in June 2022 and, at a maximum, no longer than six months after the regulations come into force.

We note that a longer grace period for Travel Rule implementation may interact with the Temporary Registrations Regime (TRR), which will now last until March 2022 following the extension earlier this year of the deadline for cryptoasset businesses carrying out cryptoasset activity in the UK to register with the FCA. While we recognise the importance of thorough FCA consideration of cryptoasset business applications, this extension places an additional burden on

the banking and finance sector to assess and manage the risk from cryptoasset businesses whose applications have yet to be approved.

We also recommend that this grace period should include consideration of developments in cryptoasset products and services, to ensure that the emerging technological solutions address emerging risks and are workable for legitimate business models. This should include NFTs, as addressed above in our comments under Q.12.

Cryptoassets: Use of provisions from the 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?

In general, we agree that new cryptoasset sector requirements should not fall below the FTR requirements for money/fiat currency transfers and not introduce new obligations on relevant persons to obtain additional CDD information above the requirements under the MLRs. That said, as the risks and movement patterns associated with cryptoasset transfers differ from fiat currency transfers, we are of the view that the UK requirements in relation to cryptoassets should be aligned to EU proposals which treat cryptoasset transfers as higher risk and therefore do not permit lower levels of information to accompany domestic transfers.

It should be made explicitly clear that personal document number (National Identity Number), date and place of birth does not need to accompany every cryptoasset transaction, but may be used as a substitute to missing Payer (Originator) address.

Section 6.15 of the consultation should be clear that the beneficiary VASP is only required to verify the accuracy of the beneficiary information if CDD was not already performed. Meaning, it should align with Article 7 Section 5 of the FTR which assumes that the verification requirement can be assumed if the beneficiary is a business relationship that was already verified as part of CDD. This wording has also been introduced through the Amending MLRs 2019, SI No. 253.

The last statement in 6.15 presents an unworkable solution, requiring manual intervention for every transfer. If this is the intention, then this will be a major change to FATF Recommendation 16 (relevant section copied below for reference) and more stringent than the FTR which will require significant resources to implement (e.g. to compare and review misspellings, truncated names, informal names vs legal names) but limited risk benefit. As per below, FATF Recommendation 16 only requires Beneficiary FI to detect missing information and verification of beneficiary information is only required if not previously verified.

Instead, as above, the PSP of the beneficiary should be able to rely on the CDD it has performed, alongside its monitoring for missing or meaningless information within funds transfers.

Cryptoassets: Provisions specific to cryptoasset firms

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

Requirements around the Travel Rule should be proportionate to the risks the legislation is seeking to mitigate, and we have considered whether the heightened risks of cryptoassets may justify a lower threshold than used for the FTR. On balance, we consider that the proposed value threshold is appropriate, as roughly equivalent to both Singaporean requirements and proposed European Union requirements (S$1500 or ~£869 and E 1000 or ~£854).

However, given the increasing use of cryptoassets across fraud and other crime types, we recommend that this threshold is kept under active review. For example, given the significant

increase in cryptoasset investment fraud, it should be noted that roughly 20% of investment scams considered by signatories to the voluntary code for Authorised Push Payments were for payments under £1000.

However, as noted above, the introduction of a "GBP" denominated threshold instead of a "EUR" denominated threshold risks creating unnecessary international fragmentation as well as intra-UK fragmentation where the UK continues to adopt "EUR" thresholds in relation to fiat payments as part of the onshored Funds Transfer Regulation.

On this note, we query whether placement of Travel Rule obligations for VASPs within the MLRs is more appropriate than placing these obligations within the FTR, whose content these obligations are replicating. Noting the "difficulties" mentioned in paragraph 6.7 of the consultation, we nonetheless suggest reconsidering whether the application of the Travel Rule to VASPs is best implemented via the MLRs. In our view, doing so creates unnecessary regulatory dispersion, unless the current FTRs applicable to fiat funds transfers could also be integrated into the MLRs, creating a consolidated MLRs incorporating all FTR requirements applicable to PSPs for fiat and crypto transfers. This would have benefits in terms of simplicity for relevant persons that are also PSPs. The current split of the obligations covered in the Transfer of Funds (Information on the Payer) Regulations in Part 7 of the MLRs, and the FTRs, does not have a clear rationale post-Brexit.

We also consider that Travel Rule requirements should leave the door open for different ways of operationalisation.

One example is the Travel Rule Protocol certain banks are members of (www.travelruleprotocol.org). The current process is that the originating VASP queries the proposed beneficiary's blockchain address (as obtained from the client) with a whitelist of VASPs until one of them confirms that the address is managed by them. The beneficiary's VASP then confirms the beneficiary name (as per the CDD record) back to the originating institution, so that the latter can perform transaction screening. The originating institution then sends a packet of info to the beneficiary VASP including originator ID, beneficiary name and blockchain tx hash.

This results in a better risk management outcome because the originator institution has a much more accurate beneficiary name to screen (since it reflects the CDD record of the beneficiary institution). There is also an operational benefit in that the beneficiary institution does not have to perform a reconciliation between the beneficiary's name as given by the originator (which may be inaccurate) and their internal CDD record.

The above approach is just one example, demonstrating that given the VA industry has a blank slate on how best to implement Travel Rule, we should be given the flexibility to adopt different models if they offer improvements on the way the travel rule works in the fiat world.

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?

Yes. We agree with this proposal.

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?

Some members believe cryptoasset transfers to or from unhosted wallets should be treated as higher-risk transactions and should be subject to enhanced scrutiny. They believe, beyond FATF

Recommendations, the UK Government should aim to set higher standards following the lead of other countries, such as Switzerland and Singapore who have already introduced stricter controls.

The Swiss Financial Market Supervisory Authority imposes stricter requirements on transactions above 1,000 Swiss francs involving unhosted/private/external wallets. Such transactions are only permitted from and to external wallets if these belong to one of the institution's own customers. FINMA-supervised institutions are thus not permitted to receive tokens from customers of other institutions or to send tokens to such customers if the information about the sender and recipient cannot be transmitted reliably in the respective payment system. Unlike the FATF standard, this established practice applies in Switzerland without the exception for unregulated wallets and is therefore one of the most stringent in the world. Transactions between customers of the same institution are permissible. A transfer from or to an external wallet belonging to a third party is only possible if, as for a client relationship, the supervised institution has first verified the identity of the third party, established the identity of the beneficial owner and proven the third party's ownership of the external wallet using suitable technical means.

If the customer is conducting an exchange (fiat-to-virtual currency, virtual-to fiat currency, or virtual-to-virtual currency) and an external wallet is involved in the transaction, the customer's ownership of the external wallet must also be proven using suitable technical means. If such proof is not available, the above rules for payment transactions apply.[1]

The Monetary Authority of Singapore (MAS) does not require payment service providers to apply Travel Rule requirements to transactions to unhosted/private wallets, but does require payment service providers to recognise that such transactions may present higher ML/TF risks, and apply appropriate enhanced risk mitigation measures[2].

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?

No additional areas have yet been identified.

ANNEX A

Areas of consideration for regulatory change

There are a number of areas within the existing regulations where we believe the current drafting, or lack of clarity regarding the current drafting, is promoting disproportionate application of obligations across industry.

Considering the focus on ensuring the removal of low value or prescriptive activity from the UK's AML regime, we encourage introducing the amends below to realign obligations towards a more proportionate application of intended AML/CTF measures.

1. Enhanced Due Diligence (EDD)

a. EDD mandated measures

[1] https://www.finma.ch/en/news/2019/08/20190826-mm-kryptogwg/

[2] Guidelines to MAS Notice PSN02, section 13-7, https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Guidelines--to--Notice-PSN02-on-Prevention-of-ML-and-Countering-the-Financing-of-Terrorism.pdf

The existing obligation in the MLRs under Reg 33(3A) is not sufficiently risk-based, in that the MLRs mandate the same EDD measures regardless of the assessed risk posed by the customer. In many situations, these EDD measures (including, for example, enhanced ongoing monitoring, establishing Source of Wealth of the customer and the customer's beneficial owners, obtaining senior management approval for establishing and continuing the Business Relationship) are disproportionate to the AML/CTF risk posed by the client as identified by the firm.

This is promoting a rules-based approach. Although firms are permitted to adjust the intensity of the EDD measures along a spectrum of risk (as per the JMLSG), each EDD measure must still be applied. As such, this clarification in the JMLSG (although welcomed by firms) is not sufficient to drive a truly risk-based approach, resulting in inefficiencies across the sector.

This links to the points made in our CfE response, highlighting the FATF Recommendation 19 messaging calling for countermeasures against black-listed countries, contradicting with the UK's approach, reflecting and requiring EDD on both the grey and black-lists. The practical impact of this should not be overlooked; for one bank, the addition of Cayman Islands alone would require an additional c.50 FTE. Recent discussions amongst member states have also highlighted concerns around the deficiencies of the HRTC regime that the UK has transposed, and is looking towards an approach that is focused on issuing guidelines on trends and typologies of transactions at risk for EU obliged entities, rather than listing third countries. As a result, there needs to be a review of the approach to HRTCs more generally, and the implementation of an approach allowing EDD measures based on an assessment of the threat posed by each country, the cost of implementation across the regulated sector and the potential unintended consequences.

As a starting point, a more proportionate, risk-based approach would be reflected if the drafting under Reg 33(3A) stated "the enhanced due diligence measures taken by a relevant person for the purpose of paragraph (1)(b) may include" rather than "must include."

Additionally, recent guidance received from the FCA to a trade association regarding HRTCs indicated the FCA's view that Regulation 33(1)(b) does not have retrospective application, i.e. the mandatory EDD only applies to customers onboarded at the time the country in which they are established is listed in Schedule 3ZA.

As a result, we believe the MLRs should be updated accordingly to reflect this, by replacing 33(1)(b) "in any" to "when establishing a business relationship:"

> *"b) when establishing a business relationship with a person established in a high-risk third country or in relation to any relevant transaction where either of the parties to the transaction is established in a high-risk third country."*

b. Enhanced Due Diligence for Politically Exposed Persons (PEPs)

PEP EDD measures are applied on the PEP if they are a customer in their own right, or a beneficial owner. The MLRs do not currently make it clear that the PEP EDD measures are not triggered in relation to deemed beneficial owners.

For example, if a client is a government entity/state owned entity (such as a central bank) there will inevitably be no BO, however the deemed BO will hold a prominent public function. Applying EDD in this low-risk relationship does not seem to be what was envisaged by these requirements.

Whilst the FCA guidance 2.40 on PEPs does allow firms to take an RBA to CDD/EDD for PEP BOs, the MLRs are silent on the matter, and should be updated for clarity.

We propose the MLRs are updated to align themselves towards the steer provided in the FCA guidance, that PEP EDD measures are not triggered in relation to deemed beneficial owners, and that this may be determined on an RBA.

c. Enhanced Due Diligence in HRTCs

The current approach with regards to the mandatory application of EDD for HRTCs does not result in a proportionate, risk-based response to the risks presented by activity in HRTCs. This is particularly demonstrated when considering the mandated application extra-territorially, within branches and subsidiaries themselves located in high-risk jurisdictions. This could be interpreted as all customers of branches or subsidiaries based in HRTCs required to be treated as high risk, bringing about concerns of operational viability and disproportionality, with low risk, legitimate customers being scrutinised regardless of the risk they pose to society.

The current obligation to apply EDD to domestic clients of HRTC generates an administrative burden and takes the first and second lines of defence's focus away from the true high-risk clients. One bank noted a 1000% increase in cases in one of their overseas branches, since the mandated extra-territorial application obligation has been in place.

EDD measures should be commensurate to the client's risk profile, rather than being mandatory across the board, to avoid directing resource towards this low value activity.

We recommend the removal of mandatory EDD for branches and subsidiaries themselves based in HRTCs, in favour of a more proportionate risk focused approach, based on an individual determination basis.

d. Enhanced Due Diligence: Complex or unusually large transactions

Enhanced due diligence requirements have been extended from scenarios where transactions are "complex and unusually large" to those that are "complex or unusually large" under Regulation 33(1)(f).

Whilst it is reasonable to monitor a client that has been flagged by the system as undertaking an unusual transaction, it can generate unnecessary workload, especially in the scenario that this transaction is a unique event with a reasonable explanation.

It would be more effective to apply enhanced monitoring when the complex or unusually large transactions are detected on the same client for a second event, becoming repetitive behaviour, which would then trigger enhanced monitoring for a given timeframe to ensure there is no suspicious activity.

Further, as the objective meaning of the term "complex" is challenging to establish (anything in the financial services sector could arguably be considered "complex" by an individual in a non-banking profession), the common-sense interpretation of the term "complex or unusually large" is such that a "complex" transaction in the sense of Regulation 33(1)(f) is in fact already treated as "unusually complex", we would suggest amending the phrase "complex or unusually large" to "unusually complex or unusually large" to make explicit this reasonable interpretation.

e. Correspondent Trading Relationships

There is limited value in automatically applying EDD on principal-to-principal correspondent trading relationships, where there is limited risk mitigation for added administrative burdens. EDD should be

limited to scenarios where the respondent's relationship with the firm is used to facilitate activity for their underlying customers, or where customer risk in the principal-to-principal relationship is assessed by the firm as high.

This is distinct from the amendment introduced last summer, clarifying that the requirement to perform EDD on the grounds of non-UK correspondent relationships applies to firms with correspondent relationships involving the execution of payments. This would be a further relaxation, for where there is a principal-to-principal relationship.

To align this requirement back to the risks, we recommend relaxation of the EDD application, so that correspondent trading relationships are only triggered when a financial institution is acting as an intermediary for their underlying customers and involving the execution of payments.

Furthermore, we would like to clarify with HMT the below:

- Clarification regarding intended definition of "third country" under Regulation 34(1);
- Introduction of a definition for "involving the execution of payments" for correspondent trading relationships under Regulation 34; and
- Clarity regarding the wider definition of correspondent relationship, considering Correspondent Banking Relationship (which is a product), Correspondent Trading Relationship and Correspondent Securities Relationship all differ, and clarity regarding the risks posed and the level of due diligence required for each.

2. Correspondent Banking Relationship definition

Currently not all actors, including new entrants, that offer services akin to correspondent banking are being picked up by the definition of correspondent banking relationship.

We believe the definition of correspondent banking relationship should be broadened, to reflect the increase in Non-Bank Financial Institutions and FinTechs who are now offering services without the formal regulatory oversight.

We request the same rules for all parties through the broadening of this definition, to ensure that all new entrants within the perimeter are required to comply with these requirements. This would not include third country AISPs as they are not involved in the execution of payments.

3. Pooled Client Accounts

The MLRs 2007 automatically offered pooled client accounts simplified due diligence application by banks. The MLRs 2017 updated Regulation 37(5)(a) to require pooled client accounts to be subject to Simplified Due Diligence (SDD) only where business relationships are deemed low risk. However, the MLRs do not define what due diligence measures can be applied to pooled client accounts.

This becomes particularly disproportionate for those customers that are not relevant persons under the MLRs and are therefore, deemed too low risk to require regulation, yet undergo stringent risk assessments to be able to continue operation of their pooled accounts.

The MLRs offer no explanation for what Standard or Simplified Due Diligence means practically for pooled client accounts. This gap was previously filled by the EBA's guidelines, which are disproportionate, impractical and have resulted in the access to banking issues we have today. The production of updated JMLSG guidance has had limited practical impact because of the constraints of having to take account of the EBA's guidelines (EBA/GL/2021/02 section 9.16ff) of additional

guidance, with sectors traditionally using client accounts noting the more stringent risk requirements continue to impact the offering and availability of these accounts.

Whilst JMLSG has since been updated to provide clarity on the treatment of these accounts, members note that there has been limited practical impact of this additional. This stems from the requirement to take account of the ESA guidance which greatly restricted use of SDD and introduced the requirement to treat all persons whose funds are held in the PCAs as beneficial owners.

Post-Brexit, some members would recommend consideration of realignment back to the requirements under MLRs 2007, to allow proportionate treatment of these accounts, and help alleviate access to banking concerns.

This would involve extending the use of SDD measures set by the ESAs beyond the very limited set of circumstances, with firms treating PCAs held by regulated firms in higher risk situations as 'light touch' correspondent relationships (i.e., banks will need to assess the customer's AML/CTF controls), linking into the conversation around monitoring or preventing risk from entering into the system.

In relation to regulated sector entities who wish to access a pooled client account, we view the introduction of obligations to identify and verify underlying beneficiaries of funds in a pooled client account in the event of a relationship rated anything other than "low" risk as a strong indictment of professional body supervisors' capabilities. We would prefer to instead establish an approach that did not lead to UKF members essentially acting as a secondary supervisor for regulated sector entities.

If existing provisions are retained, consideration should be given to aligning the meaning of the term "persons on whose behalf monies are held" with the definition of "beneficial owners" in Regulation 5 to limit the severity of current obligations in any situation other than a low risk relationship.

We would note that under the 4MLD the 25% beneficial owner threshold was removed, meaning that all beneficiaries of a trust are beneficial owners, regardless of the materiality of their interest in the trust capital/income and regardless of whether they are discretionary or vested beneficiaries. Again, as above, the review of the MLRs post-Brexit is an opportunity to review the position which is currently driving low impact activity. (Regulation 6.1c)

4. Treatment of Politically Exposed Persons

There are a number of instances, listed below, where inconsistencies between the approach set out between the FCA's guidance on PEPs, the FCA's SYSC guidance and the MLRs is causing confusion and fuelling low value activity across industry. It is entirely detrimental for guidance to be published that contradicts or differs from other guidance or regulations, as the resulting confusion and lack of clarity has huge practical impact on financial institutions.

We believe that the existing guidance documents should be revised, and aligned back to the MLRs, to promote a harmonised understanding of obligations across industry

a. Disproportionate regulatory expectations to domestic PEPs

There is tension between different regulatory expectations relating to domestic PEPs. Banks are expected to obtain MLRO sign-off for lower risk PEPS, as per FCA Guidance, but this is at odds with the requirements of the FCA Handbook. SYSC 6.3.9 requires the MLRO to have oversight over all areas of systems and controls against money laundering; it follows that the MLRO cannot (under

SYSC 6.1.4(3)) be part of an operational process within that system and control framework as the FCA Guidance requires. Further, the FCA guidance says that domestic PEPs should not be specifically reported on via annual FCA REP-CRIM obligations.

There is a disconnect between the seniority of the level of sign-off required against the decision of the FCA not to require firms to specifically report domestic PEPs, and the legislative obligation to obtain "senior management", not necessarily MLRO approval.

b. Tensions between the FCA's guidance on PEPs[3] (FCA guidance) and SYSC guidance

FCA guidance defines MLRO approval as the minimum requirement for oversight and approval of lower risk PEPs (para 2.35), which is in direct tension with the FCA's SYSC 6.1.4(3) prohibition on relevant persons involved in the compliance function being involved in the performance of the services or activities that they monitor.

c. PEP relationship definitions

FCA guidance 2.21- 2.23 appears to go further than the 2017 MLRs, by stating that the PEP relationships listed are not exhaustive and contain brothers and sisters of PEPs, as well as a further reference to aunts and uncles being potentially included for higher risk PEPs. Further clarity is required around why these specific relations were called out beyond the scope of the 2017 MLRs, and which further relations would fall into scope.

d. Potential tension between FOS complaints and FCA guidance

The FOS has been granted jurisdiction for complaints from individuals who consider that they have been disadvantaged by misidentification as a PEP or by disproportionate treatment following correct identification as a PEP. Complaints of alleged misidentification as PEPs could be fuelled by the lack of clarity within the FCA guidance to begin with (e.g. family members).

e. International implications

FCA guidance includes criteria for lower and higher risk PEPs, but we consider that some of this criteria is not straight forward to apply outside of the UK. For example, in jurisdictions such as China, the equivalent title to MP produces results in the thousands, often with no significant influence or exposure to grand corruption risk.

5. Treatment of Domestic PEPs

In addition to the points above, any review of PEP obligations needs to give mind to introducing a true risk-based assessment of PEPs, outside of mandatory EDD, that allows for a more tailored approach to individual scenarios.

A risk-based assessment of PEPs would be further enhanced by introducing a more nuanced approach to the treatment of domestic vs. foreign PEPs, in order to reflect the differing risk profiles presented. This amended approach would bring this approach in line with FATF Recommendation 12.

There should be enough flexibility introduced to allow for a true risk-based assessment of a PEP's susceptibility to corruption, and the measures in place to prevent it. This would allow low risk

[3] FG17/6: The treatment of politically exposed persons for anti-money laundering purposes

instances, such as serving UK politicians, to not have to face disproportionate EDD measures. However, this would also ensure that in the presence of additional risk factors, scrutiny could be increased accordingly, and would allow for a tailored assessment based on the risks presented by an individual customer.

This supports the discussions set out in the CfE response, around the drive for effectiveness. The cost to industry of conducting mandatory EDD on domestic PEPs far outweighs any AML/CTF benefit, as demonstrated by the absence of any prosecutions of domestic PEPs for grand corruption.

We believe this should be built into any revised PEP guidance, and the relevant flexibility reflected within the MLRs.

6. Beneficial ownership

a. BO vs PSC definition changes

There remains a misalignment between the definition of Beneficial Owner under the MLRs and People with Significant Control (PSCs), and the registration requirements for PSCs which may include legal entities and not a natural person/individual.

Alongside the lack of clarity introduced, these conflicting definitions in turn generate unnecessary discrepancy reporting obligations, draining resource that could be applied to higher priority areas of compliance.

The definition of PSC should therefore be aligned to that of Beneficial Owner.

b. Controlling Information

The current MLR approach duplicates the fit and proper person due diligence and controls as part of the licensing processes undertaken by the regulator.

It would be helpful to introduce a risk-based approach to SDD when determining beneficial ownership controlling information for financial institutions regulated in equivalent jurisdictions.

c. Regulation 5

The reference to “significant control” under Regulation 5 could be tightened, as it is not referenced elsewhere within the MLRs.

It would be useful to reiterate this under Regulation 28 and other CDD measure regulations, to make the treatment of significant controllers vs beneficial owners clearer.

7. Record Keeping

The existing requirements regarding record keeping within the MLRs deviate from FATF requirements, by going further than required.

Regulatory requirements to retain customer identification documents and supporting records, for 5 years from the date the customer relationship has ended, have been in place since the Data Protection Act (DPA) came into force in 1998. However, the DPA states that data should not be kept for longer than is necessary for the purpose it was intended.

Both the DPA requirements, and core MLR 2017 requirements, follow FATF Recommendation 10, which states that regulated firms should retain all necessary KYC records for at least 5 years after the business relationship or occasional transaction has ended. The MLRs also follow FATF Recommendation 10 in only requiring records of transactions within a business relationship to be retained for at least 5 years after the transaction.

4MLD departed from FATF standards in requiring deletion of personal data after a defined retention period. This rigid requirement for deletion is also in tension with GDPR, which is more flexible. 4MLD also departed from FATF standards in requiring retention of records of transactions within a business relationship for at least 5 years after the end of the business relationship.

The MLRs 2017 added the undernoted requirements:

- In addition to retaining customer identification documents, firms must have sufficient supporting records to enable transactions to be reconstructed (whether occasional transactions or transactions within a business relationship).
- 5 years after the business relationship has come to an end, any personal data contained in the records must be deleted.
- 5 years after an occasional transaction is complete, any personal data contained in the records must be deleted.

The MLRs 2017 also introduced the following exceptions to the defined data deletion periods:

- Transaction records only need to be kept for a maximum of 10 years from the date on which they are executed however there is no requirement to delete them after 10 years.
- Records required under another enactment.
- Records required for any court proceedings, or reasonable belief that they will be so required in future.

We believe realignment of requirements back to FATF Recommendation 10 are required, by neither requiring deletion 5 years after the end of the business relationship, nor requiring retention of transaction data indefinitely for ongoing business relationships. This would support wider discussions being held with the ICO as part of the DCMS review of data privacy regime.

Further clarity on what is meant in practice by “end of business relationship” and guidance on record retention where the customer has relationships with different “relevant persons” within a group would also be welcome.

8. Acting on Behalf Of (AOBO)

There is a lack of clarity regarding the scope of the Acting on Behalf Of requirements introduced under Regulation 28(10).

This breadth of the wording here could allow for certain scenarios to fall into scope that appear to be outside of the intended purpose of this provision.

We recommend that clarity is introduced regarding the intended scope of the AOBO provisions introduced under Reg 28(10).

9. Definition of Tax Advisor

The MLRs provide a definition of "tax adviser" under Regulation 11(d). However, this is very broad and could be read as including incidental services (for example, the provision of software that helps customers determine their tax liability). In particular, it includes the wording "assistance...in connection with tax affairs of other persons whether provided directly or through a third party".

This introduces a very broad definition, and one that brings into scope a broader range of tax advisor services than we believe were intended by these provisions.

We recommend the introduction of clarity around the scope of this provision, in particular to confirm whether it is the intention of the regulations to capture those providing software to help individuals to determine their tax liability.

10. Regulated Markets

The regulations have expanded the obligation to publish a simplified prospectus also to SME Growth Markets under Regulation 3.

With the MLRs specifically referring to the disclosure requirements for the Growth Market, it is unclear whether this impacts the categories of stock exchanges which can be considered as Regulated Markets.

We encourage clarity around this requirement, to confirm whether the changes impact the categories of stock exchanges considered Regulated Markets.

11. Legal Duty

Following changes to Reg 27(8), firms must apply CDD measures when they must contact an existing customer in order to fulfil any duty under the International Tax Compliance Regulations 2015 (e.g. FATCA, CRS, DAC2).

There is a lack of understanding of when legal duty triggers the obligation to review Client's due diligence information and to what extent. In particular, there is a lack of understanding of whether obliged entities are mandated to engage with the client directly to fulfil these obligations, as in some scenarios there may not be a need to engage with the client because their information might be available through third party vendors, or reliable public sources.

We request clarification on when the obligation to review due diligence is triggered, the process to engage clients, and the CDD measures applied.

12. Trusts Registration Service

Following publication of the Trusts Registration Service SI, there are a number of outstanding questions regarding clarity of obligations that remain unanswered.

Regarding the reporting of ultimate beneficial owner discrepancies to the trusts register, there is currently no guidance, mechanism, or access to the register in order to check and report discrepancies. There is also no understanding of details regarding expectations of extra-territorial application of trust beneficial ownership discrepancy reporting obligations, registration requirements, definition of a discrepancy, the process of discrepancy reporting alongside other practical considerations.

We encourage the production of guidance from HMRC to clarify these outstanding questions regarding the practical implementation of trust registration service obligations.

13. Further areas of the MLRs requiring clarity

There are additional areas of the MLRs where we believe the regulations, and subsequent successful practical implementation of regulations, would benefit from additional clarity. These include:

- Introduction of a definition of “business relationship” under Regulation 4(1);
- Clarification regarding intended definition of “ultimate control” under Regulation 5(1)(a);

14. Bank Account Portal

This SI consultation does not reference the removal of the requirements relating to the implementation of the Bank Account Portal. Since the HM Treasury confirmation that the UK will not be proceeding with introducing this requirement, the relevant provisions introduced under Part 5A should be removed accordingly for regulatory clarity.