5MLD consultation response

24 June 2019

Executive Summary

UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms, we act to enhance competitiveness, support customers and facilitate innovation.

We and our members are pleased to respond to the consultation on the Fifth Money Laundering Directive (the Directive). This response has been tested and developed through our Money Laundering Advisory Panel, (MLAP), including a number of workshops and consultation meetings with Government. As a result, this response represents the views of our diverse membership, and we hope that this is taken into account when considering the weight of evidence to this consultation. Given the importance of many aspects of this consultation, individual members may also respond in detail on the particular impact of these policy and procedures proposals in their individual organisations.

We support the Government decision to implement the changes to the Anti-Money Laundering (AML) regime set out under this Directive. We and our members are committed to working with all partners to develop a more effective approach to tackling economic crime, including through appropriate strengthening and rationalisation of AML regulatory requirements. Our response sets out where we consider that the proposed changes could help achieve this by addressing current weaknesses or inefficiencies in the current AML regime.

We also support the Government proposal to go beyond the requirements of the Directive, where justified by specific threats or where supporting a more holistic and strategic approach. Our response sets out where we support proposals to go beyond the requirements of the Directive to address fast-evolving issues, such as cryptoasset service providers. In other areas we support proposed changes as supporting wider strategic work to tackle economic crime. The banking and finance sector invests significant effort and resource into tackling economic crime, including innovative public private partnership initiatives such as the Joint Money Laundering Intelligence Taskforce (JMLIT) and the development of new partnership work such as the development of a joint economic crime plan and public-private threat assessment.

However, in some areas we consider that the consultation proposals need further work to align with this emerging strategic approach. Some of the consultation proposals neglect opportunities to

rationalise the current patchwork of interrelated and overlapping regulatory requirements. We consider that this is a missed opportunity, as the last few years have seen a continued influx of regulatory change projects that has placed increasing operational burdens on firms' regulatory compliance and operational teams, with comparatively little benefit in terms of the overall effectiveness of economic crime prevention. For example:

- The consultation proposals do not address all of the lessons learnt from the implementation of the Money Laundering Regulations 2017 (2017 MLRs). We were surprised to see that the consultation proposals went beyond the requirements of the Directive in some aspects but did not address other practical issues we have been raising with the Government and the Financial Conduct Agency (FCA) since 2017. On Politically Exposed Persons (PEPs), for example, the consultation does not address known practical issues including tensions between the 2017 MLRs, FCA guidance on the treatment of PEPs and FCA guidance on Senior Management Arrangements, Systems and Controls (SYSC). We encourage Government and the FCA to consider these longstanding issues and have flagged our concerns and proposed resolution within our response. We note the excellent progress that has been made on pooled client accounts thanks to the dedicated engagement of public and private sector representatives over the last year, and urge the Government and the FCA to reflect on this when considering addressing other outstanding issues stemming from the 2017 MLRs.

- We welcome the Government's decision to extend this consultation beyond the requirements of the Directive to address wider money laundering and terrorist financing risks associated with cryptoassets. We have however, identified a number of other sectors that we believe should also be considered, either as obliged entities or as otherwise incentivised to contribute to the UK's wider integrity and security regime, particularly the Telecommunications and Social Media sectors. We have provided some analysis within our Annex.

- The consultation proposals for enhanced due diligence (EDD) for EU-designated high-risk countries need to be far more holistic, otherwise there will be unintended consequences. While welcoming the Government's recognition of the potential for unintended consequences for dual nationals, our members have wider concerns about the risk of unintended consequences from definitions here being set too broadly. This could introduce excessively onerous requirements, disproportionate to the risks themselves, on both obliged entities and customers. We continue to work with our members on financial inclusion and vulnerable customer issues, and a disproportionate approach to high-risk countries would exacerbate

existing challenges for some categories of customer (e.g. certain embassies and money service businesses (MSBs) involved in cross-border payments).

- We also consider that a more strategic approach should be taken to develop the proposed reporting of discrepancies in the Companies House register. As financial sector controls have been tightened, we have observed criminals exploiting weaknesses in the current Companies House regime, so support the ambitions for wholesale Companies House reform. We have publicly advocated for public sector verification of beneficial ownership information on the Companies House register. We support the Companies House consultation proposals to develop its powers, standards and capabilities to those expectations set out in the Financial Action Task Force mutual evaluation report (FATF MER), as well as wider considerations of effectiveness in the fight against economic crime. The 5MLD consultation proposal overlaps with a related Companies House consultation proposal, currently also out for response. It is crucial that the overlapping proposals are aligned, and that all relevant stakeholders are involved in ongoing discussions, in particular to be consistent with the approach being taken in the development of the Economic Crime Plan. Not least, there is already a tension that this 5MLD consultation is proposing reporting of discrepancies around beneficial ownership information, whereas the Companies House consultation proposes that this new reporting requirement be extended to reporting of discrepancies across all customer information. It is unclear why this interdependency was not highlighted in the 5MLD consultation, as the Companies House proposal goes beyond the requirements of the Directive. We consider that the two proposals will need to be developed holistically to provide effective and workable requirements. We also consider that these proposals could support more effective public / private partnership approaches but should not be used as an excuse for private sector entities to hold responsibility for resolving data quality issues within Companies House itself.

We welcome the engagement till date with HM Treasury (HMT), the FCA and other relevant public sector bodies on the consultation proposal to introduce a central bank account register and look forward to continuing this engagement as proposals and solutions are tested over the coming months. As part of these discussions with the Government, we are developing a proposed solution that seeks to leverage existing data sources, that already collate the information required to be reported. We believe this approach would provide a compliant approach to the requirements of the Directive, and we are benchmarking our developing solution against other European jurisdictions' approaches. We believe it is crucial that the Government should ensure that all relevant public sector bodies take the time to produce an informed assessment of the potential burden of this requirement against the actual benefits that it should deliver. We need to avoid anunbalanced approach focused on more tick box regulatory adherence rather than effectiveness.

The complexities around the establishment of a central bank account register raises a more fundamental issue. Banking and finance providers are currently considering how to resource a number of strategic redesign projects, facing overlapping asks of reform and funding without a clear roadmap on how to align to a single architectural vision. For example, the reform programme for Suspicious Activity Reports (SARs) is in its infancy, building over the next few years to deliver a complete overhaul of the suspicious reporting system. Similarly, the New Payments Architecture ambitiously seeks to reform the existing UK payments system to deliver a new model for payments within the UK, including richer data and new transaction data analytics capability. Recent public private partnership developments, such as the evolving economic crime plan and public-private threat assessment, have been welcomed by members as providing an opportunity to raise the need for central mapping of the multiple operational and regulatory change projects underway. However, there is more to be done to ensure that individual consultation proposals support this strategic roadmap.

We welcome the recent close and constructive engagement between our members and HMT and look forward to continuing this to support the testing, development and implementation of the requirements from this Directive. We encourage HMT to continue to focus on effective and strategic considerations across the economic crime landscape and stand ready to continue our support of this going forward.

If you have any further queries please contact aminah.samad@ukfinance.org.uk

Chapter 2- New obliged entities

Expanding the scope in relation to tax matters

- We welcome HMT's decision to extend the scope of this consultation beyond the Directive in relation to the regulation of cryptoassets, and fully support addressing these money laundering and terrorist financing risks through regulation. There are, other sectors that members believe should be given consideration to be brought into scope of the regulations or otherwise incentivised to contribute to the UK's wider integrity and security regime. In particular, telecommunications companies and social media companies. We have attached in Annex A some detail on this.

1 What additional activities should be caught within this amendment?

- No comment on this question.

2 In your view, what will be the impact of expanding the definition of tax advisor? Please justify your answer and specify, where possible, the costs and benefits of this change.

- No comment on this question.

Letting agents

3 What are your views on the ML/TF risks within the letting agents sector? What are your views on the risks in the private landlord sector, especially comparing landlord-tenant to agent-landlord-tenant relationships? Please explain your reasons and provide evidence where possible.

- We believe that the letting agents sector is, in general, lower risk for money laundering and terrorist financing (ML/TF) in comparison to estate agents. The property market is commonly used as a vehicle to launder illicit funds, which is highlighted in the National Risk Assessment,[1] (NRA). The NRA also notes that the likelihood of criminal proceeds being laundered through estate agency services is higher than the risk of laundering through lettings services, such as rent collection. However, whilst the letting agent sector poses a lower risk of money laundering in terms of value, it is still seen as attractive for other organised crime gro[1]ups, (OCGs), especially those involved in terrorist financing, modern slavery and human trafficking. The level of scrutiny to which they are subjected should therefore be reflective of these risks.

[1]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf

- It is of equal importance that the private landlord sector, landlord-tenant direct relationships, are as responsible as agent relationships for having appropriate policies and procedures in place to mitigate ML/TF risks, including appropriate customer due diligence (CDD), training and record keeping requirements.

4 What other types of lettings activity exist? What activities do you think should be included or excluded in the definition of letting agency activity? Please explain your reasons and provide evidence where possible.

- We are happy with the proposal in the consultation to include lets only, rent collection, social housing, commercial lettings, full property management and block management as examples of lettings agent activity.

- We agree that online letting agents should be within the scope of the definition.

- The definition of lettings activity should take care not to inadvertently exclude activities that form part of a wider definition. For example, some lettings agents offer an 'introductory service' that compromises a full property management service, rent collection and other ancillary services.

5 Should the government choose a monthly rent threshold lower than EUR 10,000 for letting agents? What would the impact be, including costs and benefits, of a lower threshold? Should the threshold be set in euros or sterling? Please explain your reasoning.

- We believe the EUR 10,000 threshold is sufficient for bringing letting agents within scope for AML regulation to transpose the Directive and mitigate AML risks identified in the recitals. We do not encourage going beyond these requirements.

- We recommend that it is clarified that this requirement applies to rent per property, rather than a cumulative letting agent portfolio amount.

6 Do letting agents carry out CDD checks on both contracting parties (tenants and landlords) when acting as estate agents in a transaction?

- We believe that letting agents should be responsible for conducting CDD on both contracting parties when acting as estate agents in a transaction. We presume this is already being carried out by those lettings agents that currently offer both estate and letting services, and are therefore currently within scope of the regulations.

- There are a number of FinTech and “PropTech” companies that exist, where lettings agents outsource payment and collection activities. We recommend that these are also considered in scope as supporting industries.

7 The government would welcome views on whom CDD should be carried out and by what point? Should CDD be carried out before a relevant transaction takes place (if so, what transaction) or before a business relationship has been established? Please explain your reasoning.

- We believe that CDD should be carried out on both the landlord and tenant.

- We stress that the focus of the question should not be whether or not CDD should be carried out, but rather when it should be carried out.

- Members believe CDD should be carried out as soon as reasonably practicable after a relevant transaction takes place, or before such a transaction takes place if it is known that such a transaction is likely to take place.

8 The default supervisor of relevant letting agents will be HMRC, but professional bodies can apply to OPBAS to be a professional body supervisor. Are you a member of a professional body, and would this body be an appropriate supervisor? If this body would be an appropriate supervisor, please state which professional body you are referring to.

- We note the recent Treasury Select Committee report[2], which questioned the suitability of HMRC as an AMLsupervisor, and highlighted the fragmented approach to AML supervision that currently exists. We would stress that it is crucial that these considerations are taken into account when deciding who the most appropriate lettings agent supervisor should be.

9 What do you see as the main monetary and non-monetary costs to your business of complying with the MLRs (e.g. carrying out CDD, training staff etc.)? Please provide figures (even if estimates) if possible.

- No comment on this question.

10 Should the government extend approval checks under regulation 26 of the MLRs to letting agents? Should there be a “transition period” to give the supervisor and businesses

[2] https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/2010/201002.htm

time to complete approval checks of the appropriate existing persons (beneficial owners, managers and officers)?

- It appears that from a consistency perspective with other regulated sectors, it would be appropriate for the approval checks under regulation 26 to be extended to letting agents.

11 Is there anything else that government should consider in relation to including letting agents under the MLRs?

- We note the proposals set out for CDD obligations on pooled client accounts, including letting agents, in our response to Chapter 13. If regulation of this sector was justified, the approach to pooled client accounts would be simplified alongside existing arrangements for other regulated sectors such as lawyers.
- Where other sectors are regulated, further simplification is available for firms wishing to place reliance on a firm in another regulated sector.
- In terms of compliance and potential regulation, letting firms would be able to consider existing FinTech and "PropTech" services already live to the market and used by some financial and payment firms.

Cryptoassets

As agreed, the below is our draft response to this chapter, and we will be submitting a revised version within our agreed extension period.

12 5MLD defines virtual currencies as "a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically". The Government considers that all relevant activity involving exchange, security and utility tokens should be captured for the purposes of AML/CTF regulation, and seeks views on this approach. Is the 5MLD definition appropriate or does it need to be amended in order to capture these three types of cryptoassets (as set out in the Cryptoassets Taskforce's framework)? Further, are there assets likely to be considered a virtual currency or cryptoasset which falls within the 5MLD definition, but not within the Taskforce's framework?

- We are supportive of the Government view that all relevant activity should be captured. A level playing field in AML/CTF is important for consistency, efficiency and overall regime effectiveness.

- We are supportive of an amendment to the Directive's definition so that security and utility tokens are captured for the purposes of AML/CTF regulation.

- We note that where a digital representation of value was issued or guaranteed by a central bank or a public authority, attached to a legally established currency or otherwise possesses a legal status of currency or money, then it would be regulated as e-money. We support regulation in other cases where a digital representation of value does not meet these criteria but is still accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

- With reference to the Financial Conduct Authority's (FCA) recent draft Guidance on Cryptoassets[3], stablecoins are recognised as tokens which are stabilised by being pegged to a fiat currency. As such, the use of the wording 'is not necessarily attached to a legally established currency' may create confusion around the inclusion or exclusion of stablecoins from the Directive's definition of virtual currencies. We understand that the intent of the proposed definition is to indicate that a given virtual currency might or might not be attached to a legally established currency, rather than to suggest that no virtual currency can be tightly attached.However, we perceive no advantage to the definition to justify the ambiguity. We would therefore recommend that the Directive's definition of virtual currencies be amended to exclude mention of attachment (or lack of) to a legally established currency.

- There needs to be a distinction created between electronic monies which sit within their own (fragmented/distributed) governance structure, e.g. Bitcoin, and those electronic monies which are used as a vehicle for the transfer of other monies, e.g. Stablecoins, which would solely be the technical means by which a firm guarantees the transferability of a fiat currency. The latter should be considered simply e-money with a specific technical solution; but distinguished from stablecoins that are not pegged to a fiat currency.

- We note the challenges regulating activity where KYC information cannot be obtained (e.g. open source software freely available to download from the surface web).

- We also stress that extra-Directive scope decisions should be limited to FATF definitions.

[3] https://www.fca.org.uk/publication/consultation/cp19-03.pdf

- The Directive's definition states that virtual currencies are "…not issued or guaranteed by a central bank or a public authority"; however, there have been instances where cryptocurrencies have been backed by governments such as the petro cryptocurrency in Venezuela. The definition should be amended to remove any ambiguity and ensure this would fall in scope of the definition.

13 5MLD defines a custodian wallet provider as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies". The Government considers that all relevant activity involving exchange, security and utility tokens should be captured for the purposes of AML/CTF regulation, and seeks views on this approach. Is the EU Directive definition appropriate or does it need to be amended in order to capture these three types of cryptoassets (as set out in the Cryptoassets Taskforce's framework)? Further, are there wallet services or service providers likely to be considered as such which fall outside this Directive definition, but should come within the UK's regime?

- We consider that the Directive's definition of custodian wallet provider may need to be amended to capture services relating to security and utility tokens.

- We also support the inclusion of all types of tokens, subject to challenges noted at Q12.

- As above, we note the challenges regulating activity where KYC information cannot be obtained (e.g. open source software freely available to download from the surface web). This links to the concerns we previously raised in response to the FCA consultation over regulating non-custodial wallets, where we stated "We do not, however, support consultation proposals for AML/CTF regulation to go beyond FATF standards. In this regard we query an ambiguous recommendation from the Final Report of the Cryptoasset Taskforce[4]; namely to extend AML/CTF regulation to include "non-custodian wallet providers that function similarly to custodian wallet providers, which may otherwise facilitate the anonymous storage and transfer of cryptoassets". We note that non-custodial wallet providers are excluded from AML/CTF regulation under 5MLD and both US and Japanese regulations and consider that this seems consistent with the most recent FATF standards."

14 Should the FCA be assigned the role of supervisor of cryptoasset exchanges and custodian wallet providers? If not, then which organisation should be assigned this role?

---

4 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf

- We support the suggestion of FCA regulation, as we believe this may help to address concerns..

15 The government would welcome views on the scale and extent of illicit activity risks around cryptoassets. Are there any additional sources of risks, or types of illicit activity, that this consultation has not identified?

- We note the Egmont Group of FIUs' 2018 Typology of Virtual Currencies which identified a sharp increase in suspicious activity reporting internationally relating to cryptoassets over the past three years, with national FIUs identifying an increasing role in ML. The Egmont Group also noted that national FIUs had identified challenges associated with tracing crypto transactions, inconsistency of national regulation and number of cryptoasset exchanges operating without a license.

- We also note the JMLIT Future Threats Working Group endorses this study, and conducted a late 2018 study of scenarios for the evolution of threat of criminal abuse of cryptoassets. This identified national regulation and international regulatory consistency as key drivers for the threat.

- A report by the RAND Corporation[5] on the use of cryptocurrencies for the financing of terrorism. The findings suggest that whilst the current threat does not appear to be significantly widespread, this is likely to rise as and when cryptocurrencies gain further popularity and utility due to the anonymity and ease of creation of cryptocurrency payments and accounts. It would be best if the regulations address these potential upcoming trends.

16 The government would welcome views on whether cryptoasset ATMs should be required to fulfil AML/CTF obligations on their customers, as set out in the regulations. If so, at what point should they be required to do this? For example, before an 'occasional transaction' is carried out? Should there be a value threshold for conducting CDD checks? If so, what should this threshold be?

- We support the regulation of cryptoasset ATMs on a level playing field basis.
- We note the ongoing threat from cash-based ML/TF, with strengthened bank controls for over-the-counter cash deposits potentially leading to risk displacement into crypto ATMs amongst other routes.

[5] https://www.rand.org/pubs/research_reports/RR3026.html

- Cryptoasset ATMs should be required to fulfil AML/CTF obligations before an occasional transaction is carried out. If any value threshold were to be implemented, we suggest that this aligns to proposed e-money thresholds.

17 The government would welcome views on whether firms offering exchange services between cryptoassets (including value transactions, such as Bitcoin-to-Bitcoin exchange), in addition to those offering exchange services between cryptoassets and fiat currencies, should be required to fulfil AML/CTF obligations on their customers.

- We support regulation of crypto-to-crypto exchanges, in line with FATF standards.

- There is, however, a heightened risk of abuse identified from certain exchange services such as tumblers, mixers, etc. Such exchange services can be used by customers seeking to conceal the origin and beneficial ownership of exchanged cryptoassets and thereby undermine the possibility of customer due diligence.

- We support requirements for licensing, regulation and appropriately robust supervision and tailored monitoring of such exchange services, including the possibility of targeted prohibition of certain exchange services.

- We do not support any AML/CTF exemptions for exchange service providers, nor for customers using tumblers, mixers and related exchange services. Regulation is needed following the FCA's 2018 Dear CEO letter on cryptoassets and financial crime. This stated that:

  "Firms should assess the risks posed by a customer whose wealth or funds derive from the sale of cryptoassets, or other cryptoasset-related activities, using the same criteria that would be applied to other sources of wealth or funds… One way cryptoassets differ from other sources of wealth is that the evidence trail behind transactions may be weaker. This does not justify applying a different evidential test on the source of wealth and we expect firms to exercise particular care in these cases."

- We believe this letter understates the growing risk in this space.

18 The government would welcome views on whether firms facilitating peer to-peer exchange services should be required to fulfil AML/CTF obligations on their users, as set out in the regulations. If so, which kinds of peer-to peer exchange services should be required to do so?

- We support the regulation of peer-to-peer exchange services, such as requiring exchange platforms to obtain KYC information on each party.

- We agree that the threat from an illicit finance view is at the point of exchange and that peer to peer exchanges allow the easy layering of the proceeds of crime.

- If peer to peer exchanges were not required to fulfil AML/CTF obligations on their users, this would represent a 'weak link' and likely exploited.

- We also note the challenges in regulating peer-to-peer services provided via open source software and would welcome further guidance from government should this requirement be included.

- Regarding the type of peer to peer exchange services that should be subject to AML/CTF obligations, we believe all that the scope should be set at functionality i.e. whether users are permitted to exchange cryptocurrency. We do not believe that any exclusions based on factors such as fees would be appropriate (due to various alternate funding modes which could be implemented).

19 The government would welcome views on whether the publication of open-source software should be subject to CDD requirements. If so, under which circumstances should these activities be subject to these requirements? If so, in what circumstances should the legislation deem software users be deemed a customer, or to be entering into a business relationship, with the publisher?

- As above, we note the challenges regulating activity where KYC information cannot be obtained (e.g. open source software freely available to download from the surface web.)

- We note that the FCA, and other established regulators such as the Monetary Authority of Singapore (MAS) have taken a technologically neutral stance, and as such, we would recommend the same in this instance, where the regulations look to the activity conducted, instead of the software. We recommend that HMT look to open source software in other markets/applications, and consider similar levels of regulation in this instance. We would also urge a focus on supporting innovation, without creating inappropriate barriers to entry. We would also urge HMT to best consider how to support adoption of new technology to identify and manage AML risks, and to conduct e-ID and KYC.

20 The government would welcome views on whether firms involved in the issuance of new cryptoassets through Initial Coin Offerings or other distribution mechanisms should be required to fulfil AML/CTF obligations on their customers (i.e. token purchasers), as set out in the regulations.

- We support the requirement for regulation requiring CDD for Initial Coin Offerings, ICO, token purchasers on a level playing field basis, thereby addressing the money laundering risks associated with ICO's. Note that UK Finance members have seen increasing use of cryptoassets in investment fraud cases, including ICO scenarios.

- We refer to the stance taken by various regulators globally, such as the FCA, MAS and Hong Kong Securities and Futures Commission, where if an ICO (or securities token offering) is structured to have the features of traditional securities offerings, the offering must comply with all applicable securities laws. We would accordingly recommend that a similar approach to AML/CFT in ICOs should be taken, as is expected in a traditional securities offering, to prevent materially different regulatory requirements for similar products.

21 How much would it cost for cryptoasset service providers to implement these requirements (including carrying out CDD checks, training costs for staff, and risk assessment costs)? Would this differ for different sorts of providers?

- Without a level playing field the costs of CDD increase for other market participants, which may affect their risk appetite for the under regulated sector.

- We note that CDD costs and effectiveness will be affected by the availability of crypto specific technological tools able to mitigate the risk factors of crypto assets effectively. For e.g. tracing tools, including those able to analyse DLT for indications of interactions with the dark web and TOR, as well as product innovation in crypto assets affecting these risk factors - both negatively and positively e.g. privacy coins and tumblers, auditable information of originator and recipient, etc.

- We believe that cryptoasset service providers are in general not bound by legacy systems and are therefore at an advantage. The number of Fintech and regtech firms bringing wider KYC/CDD innovative solutions to the market in recent years also serve to advantage cryptoasset service providers. It would however be vital for such cryptoasset service providers to be provided with clear advice/guidance in respect of obligations and expectations.

22 To what extent are firms expected to be covered by the regulations already conducting due diligence in line with the new requirements that will apply to them? Where applicable, how are firms conducting these due diligence checks, ongoing monitoring processes, and conducting suspicious activity reporting?

- We note that some established credit institutions and payment service providers are / have developed their own crypto asset products and services.

- One of the key differences with how crypto CDD differs from standard is that it is not just the robustness of the on boarding controls that are relevant to cryptoassets, but whether the asset can be generated and transacted on an anonymous basis. Crypto providers and exchanges that facilitate this are much higher risk than those who do not; for those which do not offer layering of anonymisation, once the wallet owner is identified, the assets and transactions can be traced so the risks are reduced.

23 How many firms providing cryptoasset exchange or custody services are based in the UK? How many firms provide a combination of some of these services?

- The FCA's Cryptoassets guidance consultation paper[6] issued in January 2019 states in section 2.13, "there are fewer than 15 cryptoasset spot exchanges with headquarters in the UK, out of a global market of 231."

24 The global, borderless nature of cryptoassets (and the associated services outlined above) raise various cross-border concerns regarding their illicit abuse, including around regulatory arbitrage itself. How concerned should the government be about these risks, and how could the government effectively address these risks?

- We support work to promote international regulatory consistency, while noting FATF standards allow different ways to regulate the same risks presented by virtual assets; e.g. treating as commodities, treating virtual asset service providers as MSBs, etc.
- The cross -border concerns also extend to potential sanctions challenges created by the anonymisation of the ownership. In the absence of CDD/EDD this could lead to funds or economic resources being made available to targets of sanctions.

[6] https://www.fca.org.uk/publication/consultation/cp19-03.pdf

- 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.

- We support the approach to regulation going beyond the DIrective to align with new FATF standards, including an Interpretive Note to be finalised at June plenary.

- We refer to international fora such as the Global Financial Innovation Network as a potential source of cooperation in this area.

25 What approach, if any, should the government take to addressing the risks posed by "privacy coins"? What is the scale and extent of the risks posed by privacy coins? Are they a high-risk factor in all cases? How should CDD obligations apply when a privacy coin is involved?

- Privacy coins offer users complete anonymity, as compared with exchange tokens such as Bitcoin which are only pseudonymous in nature. Since an essential element of privacy coins is to mask data about their users as well as the amount traded and held in wallets, we consider the current ML/TF risks associated with privacy coins to be very high.

- It is difficult to assess the scale and extent of the risks posed by privacy coins as they are designed to reduce the evidence trail of their use.

- However, the functionality of privacy coins creates a heightened risk of abuse. Privacy coins are typically used by customers seeking to conceal origin and beneficial ownership and thereby undermine the possibility of CDD. In many cases, privacy coin marketing and product innovation show an explicit intent to undermining CDD and related technological tools.
- We support requirements for licensing, regulation, appropriately robust supervision and tailored monitoring of such services, including the possibility of targeted prohibition of certain privacy coin functionality.

- We note that CDD costs and effectiveness will be affected by the availability of technological tools able to mitigate the risk factors of crypto assets effectively (e.g. tracing tools, including those able to analyse blockchain and other distributed ledger technology (DLT) for indications of interactions with the dark web and anonymity tools such as The Onion Router (TOR)), as well as product innovation in crypto assets affecting these risk factors - both negatively and positively (e.g. privacy coins and tumblers, auditable information of originator and recipient, etc).

- Increased CDD costs and reduced effectiveness will affect firms risk appetite for business relationships involving privacy coins and related services.

- We do not support any AML/CTF exemptions for customers using privacy coins, on the basis of a level playing field, and this representing a conflict with the spirit of 2017 MLRs regulation 29(6) which notes "*The relevant person must not set up an anonymous account or an anonymous passbook for any new or existing customer*"... We consider that regulation should address implicit tension with FCA's 2018 Dear CEO letter on cryptoassets and financial crime states that "Firms should assess the risks posed by a customer whose wealth or funds derive from the sale of cryptoassets, or other cryptoasset-related activities, using the same criteria that would be applied to other sources of wealth or funds… One way cryptoassets differ from other sources of wealth is that the evidence trail behind transactions may be weaker. This does not justify applying a different evidential test on the source of wealth and we expect firms to exercise particular care in these cases."

Art intermediaries

26 What are your views on the current risks within the sector in relation to art intermediaries and free ports? Please explain your reasons and provide evidence where possible.

- The art trade is particularly vulnerable to money laundering due its cross-border nature and the involvement of high net worth individuals. The art trade typically lacks identification measures due to many individuals sidestepping the banking system to operate in cash. Artwork itself can be deliberately misvalued, counterfeited and/or stolen.It is easier for criminals to transport a piece of artwork through layers of people, institutions and borders to hide its origins than it would be for cash itself.

- As well as money laundering, terrorist groups can exploit high value goods such as antiquities by looting and selling it to raise funds for attacks. An example of this was the approach of

ISIS over the last few years. We are therefore supportive of the approach to bring art dealers into scope of these regulations.

- Free ports are conducive to secrecy and are therefore vulnerable to money laundering, terrorist financing and tax evasion. No value has to be declared to store goods in free ports or customs warehouses and they can be stored there indefinitely. They are a means by which criminals could store illicit, dual use goods or goods that should be declared for tax purposes. If goods were stored in free ports internationally they could then be shipped to the UK completely undetected.

27 Who should be included within the scope of the term 'art intermediaries'?

- The current definition should be expanded to include anyone who trades in goods as an intermediary– not only 'by way of business' – and also to anyone who is involved in a transaction for the purposes of the trade, sale or purchase of goods. This would capture those involved in a relevant transaction but who may not be directly delivering or receiving the goods.

28 How should a 'work of art' be legally defined, do you have views on whether the above definitions of 'works of art' would be appropriate for AML/CTF? Please provide your reasoning.

- Any workable definition should be proportionate whilst also encompassing priority risks. We reference the example provided under question 26, of ISIS looting of antiquities, to stress the importance of this.

29 How should art intermediaries be brought into scope of the MLRs? On whom should CDD be done and at what point?

- The current definition should be expanded to include anyone who trades in goods – not only 'by way of business' – and also to anyone who is involved in a transaction for the purposes of the trade, sale or purchase of goods. This would capture those involved in a relevant transaction but who may not be directly delivering or receiving the goods.

30 Given that in an auction, a contract for sale is generally considered to be created at the fall of the gavel, what are your views on how CDD can be carried out to ensure that it takes place before a sale is finalised? How should the government tackle the issue around timing of CDD given the unpredictability of the sale value, and linked transactions which result in the EUR 10,000 threshold being exceeded?

- As typically happens in many auction houses already, CDD could be captured upon registering with an auction house or independent auction to bid or sell. In order to capture the details of the ultimate beneficiary when somebody is bidding on a buyer's behalf – as is frequently the case with high net worth individuals who contract buyers/sellers – CDD could be required for all ultimate beneficiaries or owners before any transaction is finalised.

- With regards to the EUR 10,000, the threshold for CDD could be applied to the realistic estimate. All goods in an auction have an estimate attributed to them before the auction starts.

31 Should the government set a threshold lower than EUR 10,000 for including art intermediaries as obliged entities under the MLRs? Should the threshold be set in euros or sterling? Please explain your reasoning.

- No comment on this question.

32 What constitutes 'a transaction or a series of linked transactions'? Please provide your reasoning.

- No comment on this question.

33 What do you see as the main monetary and non-monetary costs to your business of complying with the MLRs (e.g. carrying out CDD, providing information to a supervisor, training staff etc.)? Please provide statistics (even if estimates) where possible.

- No comment on this question.

34 What do you see as the main benefits for the sector and your business resulting from art intermediaries being regulated for the purposes of AML/CTF?

- Art intermediaries being captured for the purposes of AML/CTF would ensure that activities currently being exploited will more likely be deterred, detected and/or disrupted. This would prevent illicit goods and funds infiltrating the UK financial system.

35 Should the government extend approval checks, under regulation 26, to art intermediaries? Should there be a "transition period" to give the supervisor and businesses time to complete relevant approval checks on the appropriate existing persons (beneficial owners, managers and officers)?

- No comment on this question.

36 Is there anything else that government should consider in relation to including art intermediaries under the MLRs e.g. how reliance could be used when dealing with agents representing a buyer or seller.

- No comment on this question.

Chapter 3- Electronic money

We stress that any introduced requirements within the e-money space should consider the exclusion of charity and humanitarian aid from CDD obligations over and above eligible beneficiary checks; this could otherwise bring disaster relief schemes into scope (e.g. cash vouchers which can be used in specified foodbanks).

37 Should the government apply the CDD exemptions in 5MLD for electronic money (e-money)?

- We flag that there are mixed views held across industry on this point.

- Some institutions believe the Government should apply the CDD exemptions providing the criteria has been met.

- Others believe the optional CDD exemptions in the Directive should not be applied. Whilst the obligation remains for the monitoring of transactions, if unusual activity is identified there would be no assurance that submissions to the NCA contain details of the actual person who is subject to the disclosure.

- Some members have drawn attention to the Directive also allowing member states to to prohibit payments carried out using anonymous prepaid cards.

- In addition, some members note that there should be no CDD exemptions for open-looped pre-paid cards or devices that allow for the withdrawal of cash, as per the risks set out in question 40.

38 Should e-money products which do not meet the criteria for the CDD exemptions in Article 12 4MLD as amended be considered for SDD under Article 15?

- This would be dependent upon why they would not meet the CDD exemption criteria. This could be considered on a case by case basis or further criteria set out in a specific exemption/exception for the application of SDD.

- For example, if the e-money product allowed a much higher threshold of funds to be stored electronically then SDD may not be appropriate.

39 Should the government exclude any e-money products from both the CDD exemptions in Article 12, and from eligibility for SDD in Article 15?

- We believe the threshold is still necessary for low risk products, e.g. closed loop, non-refundable cards, from a financial institution perspective.

40 Please provide credible, cogent and open-source evidence of the risk posed by electronic money products, the efficacy of current monitoring systems to deal with risk and any other evidence demonstrating either high or low risk.[7]

- Open loop prepaid cards typically pose a higher risk as they enable fraudulent merchant refunds processed, which are often credited to anonymous prepaid cards. Whilst the loading of funds to a prepaid card can be controlled by the card issuer, a credit from other means (i.e. a fraudulent merchant refund) can lead to several thousands of pounds being loaded to the card. Conversely, a card that is closed loop and can only be used at certain retailers or events (e.g. festivals) typically pose a lower risk as the funds cannot be withdrawn as cash or used cross-border.

- Higher risk e-money products could be those that are not FCA authorised but still issuing e-money in the UK via passporting permissions. Conflicts in legislation could mean controls are less stringent or subject to other jurisdictions' privacy laws which could impact UK/EU AML/CTF requirements.

- Our members are aware of cases where e-money has been used to support modern day slavery as well as terrorist financing. Some members assess crypto currency pre-paid cards as an emerging risk.

7

41 What kind of changes, if any, will financial institutions and credit institutions have to implement in order to detect whether anonymous card issuers located in non-EU equivalent states are subject to requirements in their national legislation which have an equivalent effect to the MLRs?

- This would result to a change in how financial and credit institutions operating in the UK/EU assess the AML control framework of e-money issuers from non-EU equivalent states. AML control assessments would now have to establish whether the e-money issuer has a CDD, monitoring and SAR framework that is equivalent to the MLR.

- We understand that this regulation will not have extra-territorial application and will not have impact to e.g. branches and subsidiaries outside of the EU/UK will be subject to the applicable thresholds required by their relevant regulations.

- Looking beyond legislation, MasterCard has published "AN 2625 - Identification of Anonymous Prepaid Cards" bulletin which confirms that prepaid card markers for compliant non EEA prepaid cards will be introduced later in 2019 and that all non-compliant anonymous card traffic will be blocked at the payment authorisation stage. The marker will facilitate the introduction of specific transaction monitoring rules, and we understand that other card schemes may introduce similar rules.

- The Government should recognise that such markers and monitoring rules will take time and specialist resources to design and implement. Financial institutions may still need to conduct analysis on card schemes and prepaid card issuers to determine if transaction blocking will be applied centrally or if this will fall to the card acquirer. In addition, transaction monitoring could be introduced by card acquirers to identify retailers who accept these prepaid cards, but this is likely to be difficult to achieve in practice.

42 Should the government allow payments to be carried out in the UK using anonymous prepaid cards? If not, how should anonymous prepaid cards be defined?

- There are mixed views across industry on this question. Some believe that the government should allow payments from anonymous prepaid cards if meeting the thresholds / conditions proposed in Article 12 of the Directive (e.g. Payment for goods and services subject to certain maximum limit (e.g. EUR 150)).

- Others take the view such paymentsshould not be allowed, regardless of conditions being met.If the customer/beneficial owner is not identified and verified, monitoring the transactions

will be futile because there will be no way of knowing who is carrying out the activity on the prepaid card.

- Some members believe that payments using anonymous prepaid card should only be permitted in closed loop situations i.e. store gift cards. For any open loop prepaid cards, it is suggested that Simplified Due Diligence as a minimum should be carried out on the purchaser of that pre-paid card. This could be controlled by the sponsors of that card i.e. Visa/MasterCard/AE. It would be easier for the sponsor to control either by Bank Identification Number (BIIN) range or by applying a system marker that identifies prepaid cards.

- We believe this needs further consideration by HMT, and, regardless of the decision made, we recommend that anonymous cards are carefully monitored for signs of abuse going forward.

- In addition, the definition of “anonymous prepaid card” and “type of prepaid card” need to be determined.

- The Directive specifies that financial and credit institutions acting as acquirers operating in Member States can only accept payments carried out with anonymous prepaid cards issued in non-EU countries where these countries impose requirements equivalent to those set out in the Directive in relation to e-money. It needs to be defined whether ‘acting as acquirers’ captures those institutions who are members of the credit card schemes (merchant acquirers) or institutions which effectively provide merchant acquiring services but are considered ‘payment facilitators’.

- We note that as with many other areas of EU money laundering directives, the difficulties in determining which, if any, non-EEA country “imposes requirements equivalent to 5AMLD” means that a cautious/conservative approach is likely to be taken. Further consideration should be given to the publication of an indicative list of equivalent countries or suggested methodology for making this determination; this issue with further crystalise with Brexit.

43 The government welcomes views on the likely costs that may arise for the e-money sector in order to comply with 5MLD.

- We believe the majority of these costs will be borne by those firms focusing on e-money, which in most cases will be FinTech companies (Non Banking Financial Institutions.)

Chapter 4- Customer Due Diligence

44 Is there a need for additional clarification in the regulations as to what constitutes "secure" electronic identification processes, or can additional details be set out in guidance?

- Where there is additional clarification required, we stress that this needs to be set out by Government, following which industry guidance could be produced based on the regulatory steer.

- We also note that this is a fluid area, with forthcoming FATF guidance currently being developed. It appears disconnected to be formalising a UK approach or definition, when internationally this is still being determined. The UK should be looking to the FATF guidance to guide the state of the market. This is especially important considering one of the objectives of Regulation 910/2014 is to ensure that there is a consistent approach taken cross border.

- If HMT believes "secure" must be defined now, we would suggest that key principle-based standards on "secure" should be included in the Regulations, which will set a minimum standard, but avoid any disproportionate restriction of flexibility and innovation in the market.

- Commission Implementing Regulation (EU) 2015/1502 sets out the minimum technical specifications and procedures for assurance levels for electronic identification means. If the intention is to benchmark the definition of "secure" based on certain assurance levels, this should be clearly spelled out in the approach.

- The Directive codifies the use of electronic identifications means, and secure, remote or electronic identification process for identification and verification whilst undertaking customer due diligence. The approach chosen should be clear that electronic identification and verification methods currently used in the industry will not be adversely impacted by the introduction of new guidance or standards.

45 Do you agree that standards on an electronic identification process set out in Treasury-approved guidance would constitute implicit recognition, approval or acceptance by a national competent authority?

- Where there is additional clarification required, we stress that this needs to be set out by Government, following which industry guidance could be produced based on the regulatory steer.

- Joint Money Laundering Steering Group guidance is an example of where Treasury-approved guidance would constitute approval by a national competent authority. However, there needs to be acknowledgement that this is only in relation to AML/CTF requirements only (this is the explicit remit of JMLSG). The process for public consultation and finalising JMLSG guidance provides for explicit HMT approval and implicit approval from the FCA, however it is not designed to go beyond that.

- Notwithstanding the above, the Directive permits verification of identity by means of "*any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities*". For that reason, we believe it would be helpful for any recognition, approval or acceptance to be explicit and ideally contained within a public register. We encourage Government to work with a wide range of private sector partners to develop workable options in this regard. This would be consistent with the approach being taken in the development of the Economic Crime Plan.

46 Is this change likely to encourage firms to make more use of electronic means of identification? If so, is this likely to lead to savings for financial institutions when compared to traditional customer onboarding? Are there any additional measures government could introduce to further encourage the use of electronic means of identification?

- Verification of identity via electronic means is currently widely used by UK Financial institutions due to a number of benefits including 'customer journey' and those of an operational nature. "Traditional customer onboarding" measures are usually reserved for circumstances where electronic verification measures are unable to provide required verification.

- Where future electronic verification measures are made available, the savings or costs to financial institutions would be dependent on nature of the measures and the compatibility of existing IT architecture / infrastructure.

- As technology solutions to facilitating CDD obligations are enhanced, we agree it is key to ensure the UK AML regulatory regime is suitably up to date with technological developments.

47 To what extend would removing 'reasonable measures' from regulation 28(3)(b) and (4)(c) be a substantial change? If so, would it create any risks or have significant unintended consequences?

- Requirements that include the term “reasonable measures” are generally not seen as optional across industry; instead most firms adjust the extent of their implementing measures based on the level of risk. Replacement of “reasonable measures” with another more specific term that still supports the risk-based approach might provide benefit by ensuring greater consistency of approach across financial institutions. However, it is currently unclear what more specific term would provide this balance. Furthermore, the removal of “reasonable measures” without a better replacement does move towards a rigid approach that could be seen to move towards a rule-based approach, undermining the risk-based approach to CDD.

- Undermining the risk-based approach to CDD would be a significant unintended consequence. Firms have to decide which information is gathered to meet CDD requirements dependent on the risks they have assessed; replacing “reasonable measures” seems to limit the flexibility to adapt to the level of risk and therefore the level of CDD required. This is especially true for areas such as the collection of the constitution of a corporate entity which is often viewed as an onerous obligation with negligible AML mitigation effect.

- For example, there are scenarios where a risk-based approach is necessary, such as for smaller corporate entities where senior managers identity information will likely not be available in the public domain or through electronic data providers, and where they are unlikely to exercise material influence or control.

- HMT should be mindful of adverse impacts from mandating disproportionate checks (and the additional impact of resource allocation) on areas which do not raise material AML/CTF risk.

- Removing the reasonable measures from 28(3)(b)(ii) may have unintended consequences of becoming more stringent than is required by FATF. FATF's example / expectation of 'senior management position' is the senior managing director while MLR includes the board of directors and the senior persons responsible for the operations of the body corporate. HMT should clarify the definition of senior persons and what position it would include.

- A further note to flag is that under MLR 28(4)(b), relevant persons must take “reasonable measures” to verify the identity of beneficial owners. It seems disproportionate to introduce more stringent requirements for senior managers than beneficial owners and we request that HMT clarify their expectations on this point.

48 Do you have any views on extending CDD requirements to verify the identity of senior managing officials when the customer is a body corporate and the beneficial owner cannot be identified? What would be the impact of this additional requirement?

- We note that the requirement to verify the identity of senior managing officials (when the customer is a body corporate and the beneficial owner cannot be identified) is contained within 4MLD by virtue of Article 3 (i.e. defining beneficial ownership) and Article 13 (identifying beneficial ownership and taking reasonable measures to verify that person's identity). As such, a number of financial institutions are currently adopting this approach.

- In instances where there is no individual that can be identified as meeting the definition of beneficial owner, and firms are satisfied that this is the case, we do not object to classifying the entity's most senior managing official as beneficial owner. Such an approach mirrors the obligations contained within 4MLD. Separately, we note that the term "senior managing official" has caused some confusion in the current landscape. We encourage this definition being clarified within upcoming regulation to help mitigate inconsistencies.

- We flag that there are cases where this requirement may need to be flexible to ensure new requirements do not impact the overall risk based approach. There are instances, such as with central banks, sovereign wealth funds and other publicly owned or listed entities, where there will not be a beneficial owner due to the nature of the entity, and there is a high likelihood that senior management may hold PEP status. We would be concerned that for the purposes of EDD of PEPs, these individuals were classed as "beneficial owners" rather than individuals purely exercising management/control.

- In terms of documenting this process, firms already have an existing requirement to keep records of all CDD measures undertaken, which will likely include records of the efforts made and any difficulties in establishing ownership structure. Additionally, where a firm encounters any difficulties during the verification process, consideration will be given to whether such difficulties warrant the submission of a suspicious activity report. We note that provided there is no additional requirement beyond current CDD documentation practice, there should not be an issue with this aspect of the requirement.

- There is a clear difference between a beneficial owner which cannot be identified and an entity which does not have a UBO by definition. In the latter (i.e. an entity listed on a Regulated Market) this should very clearly not be treated as a "cannot be identified" situation

and the position should remain the same as per 4AMLD/MLRs 2017 that no senior manager needs to be deemed as the beneficial owner.

- We note that this extension may create a high level of friction with any non-UK client base which could result in making the UK less attractive (noting other EU states already take this approach).

49 Do related ML/TF risks justify introducing an explicit CDD requirement for relevant persons to understand the ownership and control structure of customers? To what extent do you already gather this information as part of CDD obligations?

- In general, existing procedures already mandate institutions to understand the control and ownership structure of entity clients as part of the beneficial ownership process. In addition, risk-based measures to mitigate the risk that clients may have complex or unduly complex ownership structures, which may indicate increased financial crime risk, also capture ownership and control structure information.

- That said, under simplified due diligence, SDD, the same level of information on the entire entity ownership structure does not need to be obtained. Additionally, SDD requirements permit adjustments to the extent or type of information obtained. In light of this, risk-based flexibility would need to be maintained to avoid a material issue in this area (e.g. firms are to take ‘reasonable measures’ to establish the ownership and control structure of the customer).

- We note that generally beneficial ownership is one of the most challenging components of CDD and HMT should be conscious that removal of the term "reasonable measures" does not lead to an unforeseen impact of firms adopting an unduly conservative standard that leads to disproportionate burdens to clients in otherwise low risk areas.

50 Do respondents agree we should clarify that the requirements of regulation 31 extend to when the additional CDD measures in regulation 29 and the EDD measures in regulations 33-35 cannot be applied?

- We agree that the requirements of regulation 31 should be extended to the additional CDD measures in regulation 29 and the EDD Measures in regulations 33-35.

- Some views across industry flag that this is not a required amendment or necessary clarification.It is logical that if one cannot apply EDD then the relationship should be declined or exited in the same way as considering exit for CDD, given the AML risk is by definition

higher in any EDD scenario. Secondly, trying to determine what a “failure” to complete EDD is very uncertain and is best left to the institution taking an informed holistic view. Lastly, the required definition of the failure to apply EDD could be seen as a further erosion of the risk-based approach.

51 How do respondents believe extending regulation 31 to include when EDD measures cannot be applied could be reflected in the regulations?

- We believe an amendment to the first paragraph of 31(1) whereby regulation 29 is mentioned, with an additional paragraph covering regulations 33-35 would be appropriate.
- As above, it is difficult to try to reflect failure to apply EDD rather than leaving the judgement with the financial institution to assess within their risk-based approach. For example, a firm may be content with a less onerous EDD on an extremely low risk PEP, but apply a different standard of completeness for a higher risk client. We would encourage that the ability to maintain these gradations and nuances within application of EDD remains.

52 Do respondents agree the requirements of regulation 31 should not be extended to the EDD measures which already have their own ‘in-built’ follow up actions?

- We agree with this principle, as such internal follow up actions do not relate to potential "risk indicators" originating from the clients' behaviour. However by not specifying that any existing customer relationship must be terminated when a financial institution is unable to apply customer due diligence measures (including ongoing monitoring / periodic reviews), this may result in the unintended consequence of financial institutions permitting the continuation of relationships on a ‘risk appetite’ basis.

Chapter 5- Obliged entities: beneficial ownership requirements

53 Do respondents agree with the envisaged approach for obliged entities checking registers, as set out in this chapter (for companies) and chapter 9 (for trusts)?

- We appreciate that this requirement is being brought in for new business relationships only. We would add that this should specify that existing business relationships being reviewed as per obligations to keep CDD information up to date should also be exempted. This would also mitigate any unintended impact on otherwise eligible claimants under the Deposit Guarantee Scheme Directive.

- The requirement to check the register is an extension of the requirement in 2017 MLRs regulation 28 to verify the identity of the customer. As such, regulation 28.2(b) would apply i.e.

- *'verify the customer's identity unless the customer's identity has already been verified by the relevant person;'*

- We note that the requirement to obtain these documents should not cause detrimental impact on the onboarding of new customers. We would urge that the requirement suggests that this documentation would be subject to the existing flexibility permitted when applying simplified due diligence (regulation 37.2(a) and when opening an account (regulation 30.4) i.e.
  - *'Continue to comply with the requirements in regulation 28, but it may adjust the extent, timing or type of the measures' (37.2(a))*
  - *'The verification by a credit institution or a financial institution of the identity of a customer opening an account, any person purporting to act on behalf of the customer and any beneficial owner of the customer, may take place after the account has been opened provided that there are adequate safeguards in place to ensure that no transactions are carried out by or on behalf of the customer before verification has been completed.' (30.4)*

- Separately, we would flag the need to link this into the wider work on Companies House reform, not least to ensure that the underlying issue of registration requirements held against an unverified registry is highlighted.

- We stress the importance of recognising that the transposing regulation does not prescribe what constitutes "proof of registration on this register" or "an excerpt of the register." We consider that Government should retain this flexibility, not least because of the impact of Companies House reform on the register, including permitting application of a RBA by obliged entities. Instead, this should be addressed by industry guidance (e.g. JMLSG).

- The consultation states that the obliged entity must collect either proof of registration on the register or an excerpt of the register. This seems to assume that the obliged entity itself will be checking the register. However, in practice obligated entities will commonly rely on electronic verification solutions provided by third party data aggregators on the basis that these third parties will have (automatically) interrogated the relevant register. The transposing regulations must not be overly prescriptive as to stifle innovation and the use of such data aggregators as electronic verification sources (for example, by mandating that that an obliged entity must hold an excerpt from the register in its files).

- We welcome the Government's proposal to place the onus on the trust or company to provide proof of registration to an obliged entity, upon the obliged entity's request. As above, the

Regulation should not prescribe how the trust or company should provide proof of registration, not least because prescription stifles innovation in this space, including the use of technological solutions. We believe that HMT should be looking to promote innovation not inadvertently fetter it.

54 Do you have any views on the government's interpretation of the scope of 'legal duty'?

- We note that this should be very narrowly defined. A duty should be an obligation expressly stated in law, rather than simply a measure that an institution may wish to consider, or one of several possible measures to take; the consultations envisaged approach to "duty" does not meet this criterion.

- We do not consider that there is a legal duty to conduct CDD in the calendar year. The requirement to conduct ongoing CDD under the MLRs 2017 could include a review of beneficial ownership information, but this is based on a risk-based approach rather than mandating an annual basis.

- There are additional and potentially overlapping legal duties to review beneficial ownership information under non-AML regimes, such as common reporting standard (CRS) reporting under the International Tax Compliance Regulations. The CRS rules require that overlapping AML and tax reporting information is reasonably consistent (or there is a reasonable explanation for any inconsistency).

- We would encourage the Government to avoid over-complicating this CRS approach by creating parallel requirements to review and update overlapping information. We would suggest that any additional event-triggered review should only be required if an inconsistency was identified.

55 Do you have any comments regarding the envisaged approach on requiring ongoing CDD?

- Firms meet the existing obligation for ongoing CDD through a combination of means depending on the profile of their firm. This could include periodic reviews of the CDD on file on an ad-hoc 'trigger' basis, for example if a SAR is filed; when unusual activity is detected or where relevant information is identified pursuant to ongoing screening. Ad-hoc trigger events would also lead to wider reviews of CDD information on file pursuant to relevant changes in tax due diligence information.

- From an AML/CTF perspective, most firms would only undertake annual CDD reviews for their highest risk customers. We are concerned that the consultation proposal would result in a blanket approach which would have process, cost and system impacts (on an ongoing basis) to the detriment of customers that otherwise represent low risk from a financial crime perspective, that is not proportionate. The obligation would be better arising as part of a firm's monitoring procedures, so it is not prescriptive of an annual review, allowing it to be undertaken less frequently for lower risk customers, or when a review is triggered.

Chapter 6- Enhanced Due Diligence

56 Are there any key issues that the government should consider when defining what constitutes a business relationship or transaction *involving* a high-risk third country?

57 Are there any other views that the government should consider when transposing these Enhanced Due Diligence measures to ensure that they are proportionate and effective in combatting money laundering and terrorist financing?

- We have focused on five key issues that the Government should consider when implementing the Directive's requirements in this area:
    - The nature of EDD for high-risk third countries (HRTCs) and its relation to wider CDD requirements;
    - The risk of unintended consequences for customers if the approach to implementation undermines the risk-based approach;
    - The need to define 'involving';
    - The need to define 'business relationship or transaction'; and
    - The risk of unintended consequences for global groups and their customers if extra-territorial effects are not aligned with other relevant requirements.

The nature of EDD for high-risk third countries (HRTCs) and its relation to wider CDD requirements

- It is important to bear in mind that this part of the Directive is focussed solely on the application of prescribed (rules-based) enhanced due diligence measures. Other parts of the 2017 MLRs and the Directive apply enhanced due diligence on an escalating basis commensurate to the holistic risk posed by the customer, taking into account factors such as product and channel risk as well as geographic risk.

- We consider that Article 18 applies to circumstances where a relevant person already has an existing obligation to conduct due diligence (e.g. under 2017 MLRs regulations 4 and 27) and the customer 'involves' a HRTC. As a result, we believe that the Government implement the Directive to make clear that rules-based EDD measures related to HRTCs are to be applied only in instances where relevant persons already have an obligation to apply CDD. Our reasoning is as follows:
    - FATF's Recommendation 10 details the instances when FIs must apply CDD measures; primarily when 'establishing a business relationship' and when 'carrying out an occasional transaction';
    - FATF Recommendation 22 details the instances when Designated Non-Financial Bodies and Professionals (DNFBPs) must apply customer due diligence (i.e. casinos, real estate agents, dealers in precious metals and dealers in precious stones, legal and accounting professionals and trust and company service providers); these instances are referred to in Recommendation 22 simply as 'transactions'; and
    - FATF Recommendation 19 (counter-measures) introduces the requirement to conduct 'enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions from countries for which this is called for by the FATF'. The reference to 'business relationships and transactions' here refers back to Recommendation 10 and Recommendation 22 (i.e. when financial institutions and DNFBPs already have to conduct due diligence).

- We have seen that the risk-based approach has started to be fettered by the requirements introduced under 4MLD, such as EDD mandated for PEPs and correspondent banking. While the increased focus on these areas may have been beneficial, we run the risk of the erosion of the risk-based approach and a wholesale shift towards a rules-based approach. It is crucial the regulations are clear that even where EDD measures are mandated, there is sufficient flexibility as to how this should be conducted dependent on the underlying risk of the customer and transaction itself. As such we believe that further work will be required between HMT, supervisors and the wider regulated sector to determine how best to implement the regulations and their supervision, and stand ready to support where necessary . We address this point of targeting measures in some further detail below, under "other issues."

- We believe that this part of the Directive is implementing FATF Recommendation 19, and consider that this Recommendation supports our suggested approach:

"Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks."

- We also believe that there is no suggestion that the EU intends, through transposition of the Directive, to undermine the core FATF principle of the applicability of a risk-based approach designed to *"ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified"*.

The risk of unintended consequences for customers if the approach to implementation undermines the risk-based approach

- We believe that the Government should implement the Directive to ensure that the regulations carefully define the scope and requirements for rules-based EDD to avoid extensive and inflexible due diligence requirements disproportionate to the management of the risk itself. The definitions of 'involving' and 'business relationship or transaction' must focus on truly high risk situations arising from HRTCs, and not be so broad as to drive ineffective and inefficient 'tick box' compliance.

- Disproportionate rules-based EDD would have unintended consequences for customers due to higher administrative costs to financial institutions when engaging with such customers, through additional hurdles and delays to their access to services, or through a reduction in the range of products or services available to them. We consider that the Government should implement the Directive's requirements to ensure that customers are not unreasonably prejudiced through either the imposition of rules-based EDD unnecessarily or through rules-based EDD measures which are disproportionate to the risk.

- The risk of unintended consequences is recognised by the European Commission in its June 2018 methodology for classifying countries as high risk: '*The list does not aim at discouraging or reducing legitimate financial flows between the EU and listed third countries… Similarly, the nature of the list is not intended to have any undue consequences in third countries with regard to financial inclusion and activities related to non-profit organisations'.*

The need to define 'involving'

- The EU's HRTC regime stems from FATF Recommendation 19 which states that '*Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, <u>from</u> countries for which this is called for by the FATF' (*emphasis added*)*.

- We believe, therefore, that it would be consistent with both the Directive and FATF Recommendation 19 that the Directive is implementing, for 'involving' to be defined as 'from' a high risk third country (HRTC). We suggest that this definitions should be as follows:
    - a natural person that is resident in a HRTC;
    - a legal person that is incorporated in, or having its principal place of business in, a HRTC; or
    - a financial institution that has its main or sole regulatory authority in a high risk third country or, if such principles of regulatory authorisation do not apply in that country, is incorporated or having its principal place of business in a HRTC.
- Without a suitably focused definition of 'involving' in the implementing regulations there are many customers who would be at risk of impacts disproportionate to the risk itself. These could include:
    - a legal person with a board director that is a HRTC national or resident;
    - a UK charity with a general "worldwide" charitable purpose or that otherwise provides humanitarian aid to a HRTC;
    - a natural person who was born in a HRTC but is now a UK national and resident; and
    - a small or medium enterprise (SME) that trades with a HRTC.
- Consequently, we believe that defining 'involving' in this way we propose will enable firms to continue to focus the cost and effort burden in the areas where it is reasonable and appropriate to be identifying and managing the risk posed by a HRTC, without diverting this resource onto mandated measures for customer relationships where such risks are unlikely to materialise in practice.

The need to define 'business relationship or transaction'

- We believe that the phrase "business relationship or transaction" could lead to unintended consequences if left unclarified or defined incorrectly in the legislation. Without such a clarification, we believe there is a risk that firms, fearing regulatory censure, will take an overly-conservative approach that will result in unintended consequences similar to those seen previously in correspondent banking and PEPs. For example, a firm may apply all of the mandated EDD measures to an otherwise lower risk business relationship simply because the customer makes a single transaction to a HRTC.
- We consider that this would be disproportionate and that a risk-based approach would provide a more effective and targeted approach. As above, a single payment to a HRTC may

result in risk-based EDD measures being conducted as part of the firm's compliance with 2017 MLRs regulation 37, but we consider that the mandatory EDD measures under Article 18a of the Directive should not be applied unless the definition of 'involving' is met.

- As noted above, we consider that Article 18a of the Directive transposes (copies) FATF Recommendation 19. The phrase 'transaction' in article 18a therefore simply refers back to when relevant persons already have an obligation to conduct due diligence. For financial institutions (as well as DNFBPs) this means due diligence on business relationships and occasional transactions, as per 2017 MLRs regulations 4 and 27.

- We consider that the Government should consider the above when defining what constitutes a 'business relationship or transaction' involving a high-risk third country, in order to mitigate any unintended consequences when transposing the Directive and to ensure that the implemented measures are commensurate with the risks identified. We suggest that this definition should be made clear in the implementing regulations.

- This approach ensures that EDD remains proportionate and effective whilst minimising unintended consequences and unnecessary burden on customers, such as:

    - Students whose families are in HRTC and pay school fees;
    - Nationals of a HRTC making low level payments home for family support, e.g. NHS Doctors/Nurses resident and employed in the UK. This is particularly significant due to Brexit and the potential substitution of EU workers with citizens from other countries
    - Staff, resident or nationals, working for the UK Government (e.g. FCO/MoD), NGOs, Multinationals or as journalists in HRTC;
    - Charities generally operating in non-HRTC but which support a HRTC project on an ad hoc basis, e.g. during a period of disaster relief;
    - Manufacturing SMEs operating generally in a non-HRTC but which receive an ad hoc order from a HRTC; and
    - Transactions where intermediary banks within a payment chain, outside of the customer's control, are domiciled in a HRTC.

- If, however, Government believes that it is the intention of the Directive that the term 'transaction' includes payments across bank accounts within the context of a business relationship, these unintended consequences could be partly mitigated by splitting out the mandated EDD measures between business relationship-specific requirements from those specific to "within relationship" transactions (e.g. one-off transactions). This split should make clear that:

- the mandated EDD measures listed in Article 18a 1 (a), (b), (c), (e) and (f) should only be applied where it is the customer relationship to which the mandated EDD measures are being applied; and
- the mandated EDD measures listed in Article 18a 1 (d) should only be applied to transactions to which the mandated EDD measures are being applied.

- In addition to the above clarification of the overall phrase, we note that the 2017 MLRs do not currently define a "transaction", and the definition of "occasional transaction" is defined very broadly, as a transaction which is not carried out as part of a business relationship.
- We believe that it would be of great benefit for scope and clarity, and would reduce the unintended consequences of the current, cautious interpretation applied by firms, if a definition of "transaction" were to be introduced. The transposition of the Directive would seem an ideal vehicle to introduce one. Within the context of Article 18, this definition should be aligned with the FATF Recommendations (i.e. an 'occasional transaction' and a 'transaction' that designed non-financial businesses and professions (DNFBPs) must subject to CDD measures as per Recommendation 22).

The risk of unintended consequences for global groups and their customers if extra-territorial effects are not aligned with other relevant requirements.

- We consider that the rules-based EDD requirements related to HRTCs (for both business relationships and transactions) should not be automatically applicable to domestic customer relationships or transactions undertaken by overseas branches or subsidiaries of obliged entities that operate in HRTC locations.
- Given the extraterritorial application of UK money laundering regulations to offshore branches and subsidiaries, the Directive's requirements relating to HRTCs may lead to disproportionate impacts to firms. It does not appear operationally viable, nor effective from a risk perspective, to mandate EDD requirements to offshore offices which are based in these locations, particularly considering firms are expected to apply more stringent group level requirements to offshore branches and subsidiaries. Where this is the case, it is recommended that the branch or subsidiary of a UK financial institutions based in a HRTC does not need to apply the rules-based EDD measures on its own customers, provided that the branch or subsidiary applies CDD measures that are equivalent to the UK money laundering regulations and originating Directive (i.e. rules-based EDD measures are not required because the branch / subsidiary based the HRTC already applies measures that are equivalent to UK money laundering regulations and originating Directive, and is therefore not subject to the same AML/CTF weaknesses which resulted in the HRTC designation).

- This approach aligns with 2017 MLRs regulation 20 and regulation 33(2). We also consider that this approach would support the rules-based approach and the unintended consequences that could flow from disproportionate requirements.
- The transposing regulations should make it clear whether overseas branches or subsidiaries of UK financial institutions are expected to implement the Directive's requirements for rules-based EDD in full and, if local law prohibits them from doing so, what 'equivalent measures' should look like (e.g. as under 2017 MLRs regulation 20(3)).

Other issues

Legacy transactions

- A further point to consider is how the new EDD requirements would work for legacy transactions "involving" HRTC? If not already picked up during monitoring within this new definition, would these need to be remediated or could they be picked up by periodic/ trigger reviews? This point is also relevant to the determination for Depositor Guarantee purposes as to whether or not adequate due diligence has been performed on the eligible claimant.

Enhanced Due Diligence Measures under Article 18

- The Directive requires rules-based EDD related to HRTCs by mandating all but one of the '*examples of enhanced CDD measures that could be applied for higher-risk business relationships'* in paragraph 20 of FATF's guidance on recommendation 10 (with the addition of establishing the source of wealth of the customer's ultimate beneficial owner, which is over and above the FATF requirement). Arguably this rules-based approach, which does not take into account other risk factors such as customer risk and product risk, is in tension with FATF Recommendation 19 (which recommends that measures should be 'proportionate to the risk') and the Commission's own concerns about unintended consequences.
- The EDD measures mandated by Article 18a must therefore be aligned to a spectrum of risk, with customers whose only high risk factor being geographic risk being subject to the lowest level of EDD.
- Noting that all EDD measures must be applied, the transposition of Article 18a should permit firms to adjust the level and extent of those EDD measures in order to address the overall AML/CTF risk posed by the customer.

58 Do related ML/TF risks justify introducing 'beneficiary of a life insurance policy' as a relevant risk factor in regulation 33(6)? To what extent is greater clarity on relevant risk factors for applying EDD beneficial?

- We understand that the addition of “beneficiary of a life insurance policy” as a relevant risk factor is not an automatic trigger for EDD. We also understand that as per 2017 MLRs regulation 33(7), the presence of one or more risk factors does not always indicate a high risk of ML//TF.
- We also note that as per 2017 MLRs regulation 29 (3-5) if a relevant person is providing a customer with a contract of long-term insurance, than the beneficiaries are already identified and verified.
- Therefore, we are not opposed to the addition of this requirement into the list of risk factors

Chapter 7- Politically Exposed Persons: prominent public functions

- It comes as a surprise to UK Finance that this consultation is only focused on prominent public functions and does not address the wider issues around PEPs that are causing issues for industry, and indeed PEPs. We also note the Treasury Select Committee’s recent recommendations within this area, and Government’s decision not to pick up these recommendations.

- In particular, UK Finance has previously highlighted the below areas to Government as areas of concern:
    - Tensions between the FCA’s guidance on PEPs[8] (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.

    - Disproportionate regulatory expectations to domestic PEPs
        - Furthermore, there is a 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

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

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.
- From an extra-territoriality perspective, this would require all PEP relationships to be sent to head office for sign off by relevant senior compliance leads. Not only is this operationally unrealistic, it also leads to conflicts with local laws that may prohibit sharing customer data (even with head office.)

- 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 making 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. Due the application of mandatory measures in respect of PEP relationships, it is important that there is an exhaustive list available to firms, in order that they can appropriate manage and mitigate the burden on their customers.

- Potential tension between FOS complaints and FCA guidance
  - The Financial Ombudsman Service (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. We consider that 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). Even if FOS agrees with the determination it still costs the financial sector firm£500 to the FOS for each complaint. Consequently, we consider that the uncertainty in this area (which is encouraging complainants to go to FOS) is disproportionately burdensome on financial institutions.

- International implications

        - FCA guidance includes criteria for lower and higher risk PEPs but we consider that some of these 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.

- We have been addressing these issues with our members to seek workable solutions to mitigating these issues. The current view is that further clarity is required to avoid inconsistent and suboptimal approaches across industry, and to reduce gaps for criminals to exploit. We strongly encourage Government to clarify these issues through regulatory change.
- Alternatively, we would be happy to support roundtable discussions with industry and regulators to discuss options, such as guidance.

59 Do you agree that the UK functions identified in the FCA's existing guidance on PEPs, and restated above, are the UK functions that should be treated as prominent public functions?

- Yes, we agree with the proposal that UK functions identified in the FCAs existing guidance on PEPs are that functions that should be treated as prominent public functions.

- We appreciate the approach to transposition of the Directive, but consider that further work is required. Given wider discussions around public private threat updates and the Economic Crime Plan, we also encourage Government to support the identification of UK PEPs through providing clarifying centralised lists at suitable grades across civil service, armed forces and other relevant defined functions.

- We also note that it would be beneficial for the FCA or HMT to provide further clarity on the positions considered to be in scope outside of the UK.

60 Do you agree with the government's envisaged approach to requesting UK headquartered intergovernmental organisations to issue and keep up to date a list of prominent public functions within their organisation?

- Yes, we agree with the proposal that UK headquartered intergovernmental organisations issue and keep up to date a list of prominent public functions within their own organisation.

Chapter 8- Mechanisms to report discrepancies in beneficial ownership information

We stress the importance of the discussions on beneficial ownership within this consultation to be linked into ongoing discussions on wider company registration information within the Companies House consultation. Naturally, these requirements cannot be dealt with separately to Companies House reform and the wider economic crime reform programme. We stress the need for Government to consider and implement a robust, proportionate and sustainable model for reporting discrepancies, which is responsive to emerging threats and which manages the burden on business; both companies on the register as well as the regulated sector.

The points raised in this response relating to reporting discrepancies in beneficial ownership information would be significantly more complex if extended to all company registration information held on the Company House register, as is suggested in the Companies House consultation, not least considering the existing acknowledged problems with the reliability of Companies House data and records. We welcome recent engagement of Government colleagues with ourselves and our members to discuss these overlaps, and look forward to continuing this dialogue going forward.

One approach for Government to consider is that the measures being introduced under the Directive and Companies House present an opportunity to develop a holistic model that could meet FATF public and private sector obligations in an efficient and effective manner. Rather than adoption of siloed public-sector registries (Companies House; the PSC Register; Trust register and National Bank Account Register) which are predicated on separate parallel processes by Obliged Entities (for both CDD, Ongoing CDD and notification to public sector registries of discrepancies) there is the potential to consider adoption of a public-private sector utility which would encompass UK companies and Trusts (domestic and offshore that are in-scope for Trust registration). We would be happy to explore the details of this further with Government.

61 Do you have any views on the proposal to require obliged entities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information held on the public register at Companies House?

- It is important to note that financial institutions do currently provide feedback, although we understand that this is on the basis of saliency on a risk-based approach, with complications as below. The proposals in this chapter do not reflect a practical understanding of the current industry approach to sourcing beneficial ownership information. Common practice involves the use of third- party providers for CDD information. However, these providers themselves tend to source information from registers such as Companies House. Therefore, the likelihood of additional information being held within the private sector is not as high as suggested within the consultation. Further, where discrepancies are noted between information held on the client and that provided by the

third-party data provider, contact will often be made by the third party provider to confirm this information with Companies House, rather than by the financial institution. There is a concern that these requirements may mandate duplicative efforts across involved parties. We urge that the regulations need to acknowledge industry practice and technological options here and ensure that innovation is not stifled; particularly across third party providers delivering this service to the regulated sector.

- The chapter does not include proposals for how a new reporting requirement would interact with firms' CDD requirements, and we note that the Directive is silent on this question. We consider that the new reporting requirement should be introduced as a stand-alone requirement and not include any new CDD requirements. It is also important that the new reporting requirement does not undermine the risk-based approach and impose disproportionate burdens on standard onboarding and monitoring procedures, including simplified due diligence in low-risk business relationships, use of third-party providers and reliance on CDD information provided by another regulated firm.
- Whilst the proposal for the reporting mechanism to involve entities informing Companies House of discrepancies is generally supported, we stress that it is essential this is clearly defined to ensure that this exercise is not used as an excuse for private sector entities to hold responsibility for fixing data quality issues within Companies House itself. We note that the Companies House reform consultation sets out proposed enhancements to the way Companies House operates, including greater scrutiny of information submitted/registered for those Companies and Trusts. We note that there is already legislation in place which obliges companies and trusts to ensure information is recorded accurately at Companies House and updated in a timely fashion where changes arise, and we consider that Companies House could do more to incentivise compliance directly with companies and trusts. It is therefore important that the reporting mechanism is implemented to support Companies House reform and is not treated as extending the gatekeeping obligation to regulated firms, which would ultimately become de facto agents of Companies House. Our members also have some reservations as to the capacity of Companies House to effectively manage the potential influx of discrepancy reporting.

- Not least, criminals only need to be consistent in false information provided to obliged entities and Companies House to avoid detection, so there remains a question on how effective this mechanism is from a financial crime perspective.

- Crucial to this will be defining the scope of "discrepancy" We propose that discrepancies are looked at across three categories:

- Minor discrepancies; e.g. typos, missing hyphens;
- Discrepancies requiring further investigation, when it is unclear whether the discrepancy is material; e.g. time lags following applications to update information on the register, and other low risk anomalies;
- Material discrepancies; e.g. evidence of red flags, evidence of previously unidentified individuals.

- We propose that discrepancies are categorised across the above on a case by case basis, in line with a risk- based approach. This is crucial to ensure proportionality in reporting, to ensure avoidance of reporting discrepancies on the vast majority of companies that pose no ML/TF risk. We understand that some other Member States are taking a similarly proportionate approach to transposition of the new reporting requirement, including defining reportable discrepancies in terms of where the firm has “reasonable doubt”in the accuracy or absence of beneficial owner information on their register.

- Once categorised, all major discrepancies should be reported to Companies House within a short but practicable time frame after being categorised. The discrepancies falling into the further investigation category must also be reported within a reasonable timeframe unless discounted as typos. We note that the Directive is silent on the timeframe and process for the reporting and we consider that the new reporting requirement should support proportionate and workable approaches, such as periodic bulk reporting in the majority of cases.

- We stress that it should not be mandated that obliged entities must report the discrepancy immediately. Clarification needs to be provided regarding how quickly discrepancies are required to be reported (e.g. do they need to be reported immediately, can they be sent in bulk on a batch basis, can the approach vary by risk or some other criterion, etc). We consider that it should not be mandated that obliged entities must report the discrepancy immediately in all instances; e.g.:
    - When the obliged entity is already aware that the customer’s beneficial owners are about to change/have just changed and the customer is in the process of updating this information (e.g. management buy-out);
    - When the customer has already reported the discrepancy to Companies House but it has not yet been updated on the register.
- We believe in these scenarios, given the existing obligations for customers themselves to update Companies House, it is more appropriate for regulated firms to report discrepancies

only if and when the customer does not update the register and the regulated firm considers such behaviour material (e.g. missing beneficial ownerss) and/or suspicious.

- We note the need to manage the potential commercial and customer impacts of this proposal, whereby delays by Companies House in verifying the data in question would require disproportionate manual review and cause delay in bank onboarding processes with the customer, or indeed any other part of the customer journey. We strongly urge that discrepancies should not have any impact on onboarding once an obliged entity is satisfied they have completed the necessary due diligence; e.g. firms identifying discrepancies in low-risk customers with no impact on their risk assessment of the business relationship should be able to apply simplified due diligence. If an obliged entity is comfortable that it has identified and taken reasonable steps to verify the identity of the beneficial owner(s) (e.g. through obtaining the share register) then it has met its regulatory obligations and can proceed with onboarding, even if the register is discrepant. Commonly, the obliged entity would discuss the discrepancy with the customer and subsequently check that they have updated it. We also propose that firms placing reliance on another firms' onboarding CDD or making use of a third-party provider should not be required to duplicate the process for identifying and reporting PSC discrepancies.
- Further, the Government should take into account duplicative reporting by multiple obliged entities (and the additional, non-productive, work that will be the result for Companies House). If a 'non-compliant' flag is added to the Companies House entry it would make sense that obliged entities need not report discrepancies until that flag is removed.

- It is essential for proportionality and workability that the requirement to report discrepant information does not introduce a new obligation to check all information on the register. It is unclear why this consultation does not reference that the Companies House reform consultation includes a proposal for such a wider obligation to report all discrepancies in the register. We consider that such a wider obligation is gold plating of the Directive and that it is not justified in terms of being required to mitigate a material ML/TF risk. It must be clear that the Directives' obligation is to report a discrepancy when it is identified through the obligated entity's due diligence processes.

- Clarification is required on whether the requirement to report discrepancies is restricted to reporting the obliged entity's customer when conducting due diligence, or whether it extends to other circumstances (e.g. to the customer's parent company, or when discrepancies are identified through intelligence-based investigations such as JMLIT or court orders). In such other cases, law enforcement may already be aware of the discrepancy and may not want it to be reported to Companies House. There is also a question of efficiency. The problem of

requiring regulated firms to report to law enforcement what law enforcement already know has arisen in a number of areas and is being addressed through SARs reform. We strongly urge the Government to apply lessons learned and avoid unnecessarily and costly over-reporting.

- We also note the need to manage the potential market impacts of this proposal, whereby a lack of regulatory clarity over definitions and requirements would drive inconsistent market practice. We propose that implementation of this requirement of the Directive should include consolidated public sector guidance aligning the CDD, POCA and Companies House requirements. We also propose that HMT work with other EU Member States to encourage consistent definitions and requirements, to manage the potential for market disruption and regulatory arbitrage.

- We also note that there are a number of outstanding questions that need to be addressed by Companies House during their consultation process, including how long it would take them to resolve discrepancies considering, dependent on how this is defined, the number could be numerous; what Companies House will do with the information provided by an obliged entity; how Companies House intend to validate this information with companies, and whether Companies House would advise obliged entities when Companies House is updated.

- We recommend that HMT, Companies House and BEIS reflect on the commonalities between reporting discrepancies to Companies House and the known issues of the suspicious activity reporting regime as highlighted by the Law Commission's review of POCA (e.g. duplicative reporting, reporting what Companies House already knows, or over reporting in the absence of clear guidance).

62 Do you have any views on the proposal to require competent authorities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information held on the public register at Companies House?

- We note that it is important that supervisory authorities have access to data sources more reliable than Companies House unverified data.

- Where a competent authority (i.e. FCA or PRA) holds beneficial ownership information which differs from information contained on Companies House, we believe that it would be appropriate for said competent authority to inform Companies House accordingly.

63 How should discrepancies in beneficial ownership information be handled and resolved, and would a public warning on the register be appropriate? Could this create tipping off issues?

- We support a warning flag on the register, to be in place for the duration all discrepancies are being reviewed. We do not believe a general discrepancy flag would change the tipping off risk, not least because delays in onboarding of customers on the banking side already allude to legitimate criminals that additional reviews are being completed on high risk accounts.

- We also note the importance of Companies House reform allowing its own internal analysis and process change, so that the treatment of anomalies is not simply for Companies House to call the individual in question and repeat what they were told by the reporter.

- In terms of resolving discrepancies, it would also be crucial for there to be some sort of feedback loop back from Companies House to the reporting entity, to confirm whether the discrepancy information was valid or not. We trust that the public sector commitment ensures there is resource within the reformed Companies House structure to do this.

- Obliged entities will need to understand the service level agreements (SLA) that Companies House has to investigate and resolve a reported discrepancy. We suggest that the 'non-complaint' flag should be an indication to the reporting obliged entity that their reported discrepancy is still under investigation. Should the flag be removed without the data attributes being corrected by Companies House, it is likely that the obliged entity will have an obligation to report the discrepancy for a second time.

- We consider that may be a risk of tipping off in advance of the introduction of the new reporting requirement. Companies House already receives information on discrepancies through its 'Report It Now' facility and we understand that its standard practice is to contact the company in question to query the discrepancy.

- We consider that the new reporting requirement should not apply where firms have reported suspicions of money laundering and noted discrepancies in Companies House beneficial ownership information. In such cases there should be information sharing arrangements between the UK Financial Intelligence Unit and Companies House to allow information on the suspicious discrepancies to be shared, in support of Companies House compliance and enforcement activity.

Chapter 09- Trust registration service

We note that the proposals laid out in this chapter are cross-sectoral in nature, and are significant far beyond the banking and finance industry. We recommend that these are therefore assessed on a cross-sectoral basis. UK Finance are happy to convene engagement with our members alongside representatives from the legal, accountancy and estate agent business.

64 Do respondents have views on the UK's proposed approach to the definition of express trusts? If so, please explain your view, with reference to specific trust type. Please illustrate your answer with evidence, named examples and propose your preferred alternative approach if relevant.

- As HMT observes in paragraph 9.14 of the consultation paper, the use of trusts is more widespread in the UK than in other EU jurisdictions and many arrangements that are essentially contractual in civil law jurisdictions would be categorised as trusts under English law. It follows that there is a risk that the registration requirement has inconsistent application across the EU and that the impact on the UK is disproportionate. We are aware, for example, that in the Netherlands the application of this aspect of the Directive is restricted to one type of trust like arrangement which is the most common structure (the mutual fund - "fonds voor gemene rekening"). We fully support and indeed consider it critical that, as set out in paragraph 9.14, the government explores how equivalent arrangements are treated in other EU Member States when clarifying the registration requirements to avoid it being applied differently across the EU and the resulting compliance burden. A principled approach should be applied by the government to the trusts to be subject to Article 31, taking into account the fundamental purpose of the Directive as well as proportionality. We consider that this should entail a tightly circumscribed definition of express trusts in the UK.

- We stress that it may be of use to define what is not an express trust, for clarity around scope across industry. For example, joint tenancy agreements technically meet the definition of an express trust. Most people with joint tenancies are likely to have difficulty in applying the principles of an express trust, and many will not even be aware that they are in one, what it means, let alone that it amounts to a Trust.

- We would also like to clarify whether the Directive changes the existing obligations and responsibilities of the operator or manager to comply. For example, guidance on 4MLD implementation was issued to the industry by HMRC confirming that unit trusts are excluded from the definition of express trust and therefore no unit trusts should be within scope of the requirement to register, whether the Trustees were UK or non-UK resident.

- There could also be changes to existing obligations and responsibilities if charitable trusts were included within the definition of “express trusts”. If charities schemes approved by the Charities Commission were included, we would like to clarify whether the manager or operator of the Charity scheme is the entity responsible for ensuring adequate, accurate and up-to-date information on the beneficial ownership of the units in the scheme is held/maintained.

- We note that the use of express trusts across the banking industry results in certain types being more commonly dealt with than others. We note that across our members, will trusts or discretionary trusts are most common, largely due to the estate planning of the settlor. When looking at retail banking, the main focus was noted by some members as being on charitable trusts which are typically discretionary. There are also instances of will trusts often seen here. It has been noted that it is unlikely to see examples of testamentary trusts, those created by settlors will, transferring property into a trust on death, in the brokerage or corporate/investment banking space. Other members noted that revocable trusts, allowing the settlor to retain sole control of the trust, were rare.

65 Is the UK’s proposed approach proportionate across the constituent parts of the UK? If not, please explain your view, with reference to specific trust types and their function in particular countries.

- Rather than the UK, we note that across the EU, UK trust structures are most commonly used. As a result of this, the impact of these requirements will be inconsistent across the EU, and are likely to have a disproportionate impact on the UK in particular.

66 Do you have any comments on the government’s proposed view that any obligation to register an acquisition of UK land or property should mirror existing registration criteria set by each of the UK’s constituent parts?

- We agree that the obligation to register should be in line with the registration criteria set by each of the UK constituent parts; i.e. Land Registry.

67 Do you have views on the government’s suggested definition of what constitutes a business relationship between a non-EU trust and a UK obliged entity?

- We note the significance of the definition of business relationship, which would bring about a dramatic shift in trust registration requirements. This would require any non-EU trust which has a UK bank account or borrows money from a bank in the UK, or uses the services of a UK investment adviser, UK accountant, UK lawyer or a UK tax adviser, to register the trust details on the UK trust register.

- We stress to Government that the significance of these requirements could result in non-EU resident trustees being deterred from using the UK (and other EU) service providers. We are aware there are concerns within the trust industry that this could result in a shift away from the UK, where the trust advisory sector is highly regulated and compliant, to other jurisdictions.

- As in Q64, we note that many arrangements that are essentially contractual in civil law jurisdictions would be categorised as trusts under English law. It follows that there is a risk that the registration requirement is applied differently across the EU and that the impact on the UK is disproportionate.

- We would also like to clarify whether regulated firms would only be required to register the trusts with which they had a direct business relationship. This is important as there may not be a contractual obligation with a trust within a customer's ownership structure.

68 Do you have any comments on the government's proposed view of an 'element of duration' within the definition of 'business relationship'?

- We note that this is the first time that a view has been given at to the timescale of 'an element of duration'; which currently this is left to each relevant person to take a view. We believe 12 months is a sufficient proposed timescale.

69 Is there any other information that you consider the government should collect above the minimum required by 5MLD? If so, please detail that information and give your rationale.

- Rather than additional information that should be collected, we note requirements under 4MLD which have not been defined clearly are causing disproportionate efforts across industry when considering the risks involved. In particular, the requirement to include information on the "class of beneficiaries" is proving problematic in practice, due to a lack of clarity around how this should be defined.

- This is particularly prevalent in the capital markets space, when looking at bonds. Given how bonds typically operate, held in bearer form through the clearing system, it is often not clear who the beneficiaries are. Considering the scale and impact this has, and the low risk of AML/CTF within these products, we would stress that it would be best placed to introduce an

exemption for bonds and loans products with regards to registering “class of beneficiaries” for trusts.

- Additionally, there are issues with interpretation of trust deed documents that have not been considered within the 2017 MLRs. Regulation 28(4)(c) requires firms to try and understand a trust's ownership and control structure, with regulation 6(2) defining control as including powers to appoint and vary/remove trustees. This information should be set out in the trust deed but these documents can often be difficult to interpret (e.g. very lengthy and archaic in structure), with trustees sometimes reluctant to provide a copy. This causes significant operational difficulty to firms attempting to establish this information.

70 What is the impact of this requirement for trusts newly required to register? Will there be additional costs, for example paying agents to assist in the registration process, or will trustees experience other types of burdens? If so, please describe what these are and how the burden might affect you.

- We seek clarity on the expectations on obliged entities if discovered that a trust is not registered during the obliged entities onboarding process.

- The scale of the requirement is significant in every respect, from the due diligence required to identify express trusts, the requirement to develop and build software and manual processes to capture required information and effectively process it for registration, the additional human resources and infrastructure required and the very significant costs involved in doing so.

- As professional trustees of bonds and security arrangements our members are particularly concerned that, to the extent the trusts they administer are not excluded from the definition of "express trust" and to the extent "beneficial ownership" is not confined to natural persons in the manner suggested, they should only be required to register the "class of beneficiary" (e.g. "secured parties", "lenders", "bondholders" as the case may be.) This would not include the individual identities of beneficiaries which are very difficult to determine and to update when they frequently change, especially on a backward-looking basis. The additional burden created by the obligation to update should also not be underestimated.

- In the context of a syndicated loan, for example, the identity of a lender beneficiary of a security trust can change frequently during the life of the loan as positions are traded, necessitating an almost constant monitoring of beneficial ownership and updating of the

register. An exclusion for bond and security trusts in commercial transactions is preferable. This would also be consistent with the equivalent arrangement in other EU jurisdictions where contractual promises or security are held on behalf of a changing class of beneficiaries under a legal device which is not a trust (see the last sentence of paragraph 9.14 of the consultation paper) and thus would not require to be registered.

- English Law governed trusts are ubiquitous in European financing arrangements.It is not unfeasible that the increased burden on professional trustees to fulfil onerous registration requirements and the huge cost of doing so (which would likely be borne by investors if not the trustees themselves) could interfere with the efficient operation of loan and capital markets, impacting pricing and competition and placing undue stress on these vital markets.

71 What are the implications of requiring registration of additional information to confirm the legal identity of individuals, such as National Insurance or passport numbers?

- Requiring additional information also adds to the diligence burden and associated costs referenced in our response to question 70. Members have also expressed concerns regarding the data protection implications of being required to request and store personal data. There is potential for this requirement to interfere with other obligations under data protection legislation, such as GDPR, as well as the further additional cost of ensuring significant additional amounts of personal information is held and processed in a compliant manner.

72 Does the proposed deadline for existing unregistered trusts of 31 March 2021 cause any unintended consequences for trustees or their agents? If so, please describe these, and suggest an alternative approach and reasons for it.

- We note that the requirements are significant and will therefore result in significant operational efforts to implement. As a result, the timeline till 31 March 2021 may be too short for all existing trusts to be registered, and an extension should be considered. We recommend additional flexibility particularly around inputting information on existing trusts.

73 Does the proposed 30 day deadline for trusts created on or after 1 April 2020 cause any unintended consequences for trustees or their agents? If so, please describe these, and suggest an alternative approach and reasons for it.

- As above, we believe the proposed timeline is too short given the operational significance of the requirements. As a result, we believe this should be extended to 90 days.

74 Given the link with tax-based penalties is broken, do you agree a bespoke penalty regime is more appropriate? Do you have views on what a replacement penalty regime should look like?

- No comment on this question.

75 Do you have any views on the best way for trustees to share the information with obliged entities? If you consider there are alternative options, please state what these are and the reasoning behind it.

- No comment on this question.

76 Do you have any comments on the proposed definition of legitimate interest? Are there any further tests that should be applied to determine whether information can be shared?

- We note there are concerns amongst members around the data, security and fraud aspects of persons with "legitimate interest" having access to trust data. We note that further understanding is requested around:
    - Who would control access to the register;
    - How legitimate interest would be verified and re-confirmed;
    - Restrictions on data uses;
    - How restrictions would be monitored; and
    - FI obligations on keeping data up to date.

- It is not uncommon for beneficiaries to be unaware that they are named in trust deeds, and that there may be sensitivities around this information being shared too freely and widely without some protection over what legitimate interest allows

77 Do the definitions of 'ownership or control' and 'corporate and other legal entity' cover all circumstances in which a trust can indirectly own assets through some kind of entity? If not, please set out the additional circumstances which you believe should be included, with rationale and evidence.

- We believe the definitions to be appropriate insofar as including "other means of control over that entity as defined in the 2017 PSC statutory guidance on the meaning of 'significant influence or control".

78 Do you have any views on possible definitions of 'other legal entity'? Should this be defined in legislation?

- To avoid the risk of inconsistent implementation or interpretation we believe that a definition within legislation would be appropriate.

79 Does the proposed use of the PSC test for 'corporate and other legal entity', which are designed for corporate entities, present any difficulties when applied to non-corporate entities?

- No comment on this question.

80 Do you see any risks or opportunities in the proposal that each trust makes a self-declaration of its status? If you prefer an alternative way of identifying such trusts, please say what this is and why.

- Different members focused on different risks and opportunities in this proposal. Some members stressed the importance of a level playing field for all obligated entities in confirming the settlor. Some other members emphasised the importance of flexibility to accommodate the diverse uses of trusts across different markets.

81 The government is interested in your views on the proposal for sharing data. If you think there is a best way to share data, please state what this is and how it would work in practice.

- A large volume of data including personal data will be held by government and there are currently no proposals in place on protections around it. This raises the question as to whether the GDPR and other personal privacy implications have been considered and also the risk of the data being vulnerable to hacking and security breaches. Robust protections are required to address these concerns. Article 31(7)(a) of the Directive provides for exceptional circumstances to be laid down in national law where there is an exemption from such access to all or part of the information on the beneficial ownership (e.g. where the beneficial owners is a minor or otherwise legally incapable). It is unclear from the consultation paper what the exemptions will be in the UK and further detail is therefore required on this.

Chapter 10- National register of bank account ownership

We welcome the engagement that UK Finance and its members has had to date with HMT, NCA and FCA to discuss the bank account register. We stand ready to continue to provide support to the testing and scoping of requirements in the run up to the regulations being laid. We are in agreement

with public sector departments and agencies that this area is of the upmost priority, to ensure that a proportionate, efficient and effective solution is implemented.

We note the complexity of the requirements for the bank account register, and the unconfirmed status of many of its components such as scope, structure and owner. Based on this, we have developed the following analysis and proposal with members to determine the most beneficial way forward in the absence of some of these key decisions.

82 Do you agree with, or have any comments upon, the envisaged minimum scope of application of the national register of bank account ownership?

- We note the proposal by HMT to extend the scope of the register beyond IBAN accounts, as required by the Directive, to include;
    - credit and payment institutions which issue credit cards;
    - e-money issuers which issue prepaid cards; and
    - credit unions and building societies which issue accounts not identified by IBAN.

- We do not support the proposed gold plating in this area, not least because without the rationale and purpose of the register being set, there does not seem to be adequate justification in doing so. We note HMT's statement that "the government will only 'gold-plate' (go further than) the provisions in the Directive where there is good evidence that a material ML/TF risk exists that must be addressed."

- We believe that prioritising IBAN accounts would allow for law enforcement to track funds and payments in the most time critical cases (e.g. terrorism and human trafficking.) Equally there are strong examples of strong public-private partnerships already in place, such as JMLIT. If gold plating were required to go beyond IBAN accounts, we consider that further justification of this would be essential.

83 Can you provide any evidence of the benefits to law enforcement authorities, or of the additional costs to firms, that would follow from credit cards and/or prepaid cards issued by e-money firms; and/or accounts issued by credit unions and building societies that are not identifiable by IBAN, being in scope of the national register of bank account ownership?

- Currently, it does not appear that the operational significance of the implementation of the register has been appreciated, and that this is not proportionate to the potential benefits of establishing the register.

- We therefore consider it crucial that Government spend time assessing the actual benefits to law enforcement of different approaches to implementing the register, particularly for the potential gold plating.

84 Do you agree with, or have any comments upon, the envisaged scope of information to be included on the national register of bank account ownership, across different categories of account/product?

- Members have flagged the complexity of certain bank accounts, and that it is unclear how reporting information would work in these areas. In particular, in the wholesale and investment banking space, it was noted that the complexity of these customer and industry relationships and accounts meant that it would be significantly more difficult for requested information to be provided.

- A further point to note is around which type of account is more valuable for this register than others. We consider that, if the purpose of the register is for time critical access to bank information, for example in terrorism cases, then this purpose would seem more directly applicable for retail accounts. Information for retail accounts is much more readily available and exists across multiple data sources already. As a result, we note that it would be helpful to test a solution to the register across retail accounts only in the first instance.

- We flag that additional protections are required for new information demands, and that this could complicate reporting if legislation only provided protections for statutory definitions of required customer due diligence information (e.g. beneficial ownership thresholds of share holding, etc). For example, firms commonly apply lower beneficial ownership thresholds in higher risk situations. Therefore stronger protection is needed to support the reporting of broader information under a risk-based approach.

- We stress that the scope of information will need to be considered within the context of a number of issues that will have to be resolved, such as;

    - The problem of mandating a unique identifier number when there is no obligation for obliged entities to capture a unique identifier number
    - The risks inherent in mandating certain identification data (such as passport numbers) on individuals who are socially or financially excluded, or where the account holder has been verified through electronic means
    - Account holders such as listed companies and government agencies which will not have UBOs

- Account holders with multiple names (e.g. registered vs business name, sole traders)
- Account holders with UBOs that are not individuals (e.g. trusts with a 'group' beneficiary)
- Additionally, the security/safety of the data contained within a register may not be guaranteed, even if appropriate safeguards have been created; there is always a risk of a substantial database being hacked or breached with obvious adverse consequences
- Data protection/ privacy including the necessary scope of legal protections for data submitters to the BAR.

85 Do you agree with, or have any comments upon, the envisaged approach to access to information included on the national register of bank account ownership?

- We note that once again this will be dependent on the agreed purpose of the register, but do not yet see the need for regulators to have access to this information.

- We also note that we are committed to the approach taken by the UK Government to the protection of personal data and, thereby, to limiting the disclosure and circulation of such data to only those circumstances where this is appropriate and necessary to the enforcement of laws and the public interest.

- An option seen through benchmarking with other EU jurisdictions would be for the legislation to focus on the threshold criteria that law enforcement should meet in order to access the data available in this register. For example, in Germany we understand the threshold criteria to be:
  - A criminal procedure must have been officially commenced (administrative fine proceedings are not sufficient); or
  - Case of providing international judicial assistance in a criminal case; or
  - The access must be necessary (no other means of obtaining the information.)

86 Do you have any additional comments on the envisaged approach to establishing the national register of bank account ownership, including particularly on the likely costs of submitting information to the register, or of its benefits to law enforcement authorities?

- This question cannot fully be answered without a steer on mechanism or scope of the register. However, this is clearly a hugely significant operational project, which will have substantial cost, resource and technological impact across industry.

- As per our answer to question 83, we believe it is of the highest priority that Government spend the time to assess the actual benefits to law enforcement in the establishment of this register, to ensure that this is proportionate to the potential benefits of establishing the register.
- This will also allow for sufficient time to align this strategically and operationally with work underway on the beneficial ownership registers, SARs reform and the economic crime plan.

87 Do you agree with, or have any comments upon, the envisaged frequency with which firms will be required to update information contained on the register? Do you have any comments on the advantages/disadvantages of the register being established via a 'submission' mechanism, rather than as a 'retrieval' mechanism?

- Initial conversations have been discussing the options between a push or submission mechanism, versus a pull or retrieval mechanism for obtaining the required data from financial institutions. Given the lack of clarity around purpose, scope and requirements of the register at this time, it is difficult for industry to fully assess whether one of these options, or indeed a third approach, would be best placed. However, we have included some initial analysis below:

    - Push system: A push system would ensure that institutions do not have to develop new technologies or systems to align with any implemented pull system, helping to avoid excessive costs in this area, particularly for smaller and specialist institutions. However, a push system does place a manual burden on institutions to submit information frequently, which, dependent on the proposed mechanism, may itself have significant resourcing and technology implications. Additionally, a push system may result in data on all in-scope customers and accounts being stores in a database waiting for use by LEAs etc. There are significant data security and protection concerns with this, not least, the security/safety of the data contained within a register may not be guaranteed, even if appropriate safeguards have been created, and how the lawfulness of data processing can be addressed in the context of the rights of individual consumers. Additionally, the administration of a central database will also impost a heavy burden on the appointed authority

    - Pull system: Implementation of a pull system would ensure that data is accessed as and when required. This not only reduces the administrative burden on submitting firms, but ensures that data is only accessed on a necessity basis, thus reducing the potential data security and protection issues. As noted above however, this approach may well have significant impacts on firms resulting from the need to align

technological systems to allow information to be obtained. In addition, the required information is often held across a number of different systems within individual institutions, let alone across them. As a result, it could be a costly and complex solution to coordinate and align different systems to allow this information to be collated. This complexity could be reduced by focusing on IBAN accounts.

- Considering the above, we believe that there is a more efficient route to meeting the requirements of the Directive. We believe the focus should be on the workability of the final mechanism, and that going beyond the scope of IBAN accounts, i.e. gold plating the requirements of the Directive, should not be considered in the absence of specific priority threat indicators that suggest otherwise. As a result, the most effective workable solution would be to leverage existing data sources to collate / access the required information.

UK Finance Proposal

- Our position is that it would be beneficial for an initial "quick and simple" solution to be implemented for the October 2020 deadline, which makes steps towards meeting the requirements of the Directive. This would then allow, on a long-term basis, Government to undertake a detailed benefits review, and explore the potential to include added value goals, to operational and cost impact of establishing the register is proportionate to its benefits.

- To pull together this initial solution to the register, we propose that the focus is on leveraging existing data sources. During the establishment of existing filing requirements, for example Single Customer View, matters such as the differing approaches of firms to IBAN or account numbers were worked through and resolved for the purposes of generation and submission of the file. For example, banks with small numbers of accounts use their own IBAN and do not necessarily have sort codes and account numbers, whereas banks with larger numbers of accounts have individual account identifiers for each customer and/or account. Consequently, leveraging existing files in fulfilment of this Directive requirement would avoid duplication of effort and work on the part of Government, supervisory bodies and firms.

- We have identified a number of existing data sources which encompasses all or part of the data envisaged by the data, including:
    - Data sources available now:
        - Credit Reference Agencies- Experian/Equifax: Currently hold personal data; and information on credit accounts, including the date it was opened and the account

number. One proposal could be to expand the remit of these credit reference agencies to incorporate other information required by the register.
    - Open Banking; particularly leveraging API's
    - FSCS Financial Services Compensation Scheme, particularly through the Single Customer View (SCV).
    - CIFAS
    - PSC register for beneficial ownership information
    - HMRC Common Reporting Standard reporting
  - Data sources available later:
    - Confirmation of Payee (for retail banking) – the Payments Services Regulator (PSR) has announced revised plans on a direction to ensure coordinated roll-out across the industry, to ensure that the major providers of retail bank accounts go live with this service at the same time
    - New Payments Architecture – Particularly the transaction data analytics
    - SARs reform programme and the new transaction reporting proposal

- We believe that the scope of information provided collectively across these sources is in line with the requirements of the Directive. Equally, if Government believed that one or more of these sources should be enhanced to include additional data fields. From a cost/benefit perspective, it would be less burdensome on firms to add a field to existing software than it would to generate an entirely new file format.

- We flag that as discussed with public sector departments and agencies, we are working on benchmarking approaches across other European jurisdictions, the details of which are as follows:
  - **Netherlands**: The Bank Data Retrieval Portal is being developed to share customer data, with a new law being drafted that will require banks which provide IBAN numbers to its clients to connect to the portal. LEA's/FIU's etc. will then be able to retrieve customer data directly from this portal on a targeted basis following a specific request.
  - **Spain**: A regulatory requirement already exists to register bank accounts for individuals and entities, applicable to current accounts, savings accounts, trading accounts and termed deposits only. A regulatory reporting tool provided by the Bank of Spain is used to input the information that is submitted monthly to the register.
  - **Finland**: The Finnish proposal uses two separate subsystems, the first a centralised register with information on payment accounts kept at payment institutions, electronic money institutions and providers of virtual currencies. The second is a data retrieval

system which would be a technical interface allowing competent authorities to make queries and banks to provide requested information directly.

- **Italy**: We understand that a new decree on the Directive has been approved by the Italian Government. However, Bank of Italy Guidelines regarding its operational implementation are still under consultation.
- **Germany**: Banks submit information to third party providers, and public agencies authorized to receive information can access it through here. Information can only be accessed if certain criteria are met by LEA's.

- It is worth noting that these other approaches appear to be dependent on local legal and constitutional arrangements, as well as leveraging systems that already exist for other purposes.

- We consider it crucial that Government should follow suit and take a flexible approach to achieve the right outcome in a way that is appropriate and proportionate for the UK regime.

Chapter 11- Requirement to publish an annual report

88 Do you think it would still be useful for the Treasury to continue to publish its annual overarching report of the supervisory regime as required by regulation 51 (3)?

- Yes, we believe it would still be useful for HMT to continue to publish its annual overarching report of the supervisory regime, regardless of the Directive's requirements for supervisory authorities to publish their own annual reports.

- In particular, we see benefit in an overarching supervisory approach to ensure consistency across all supervisors following the concerns of the Treasury Select Committee around the fragmented approach to AML supervision in the UK.

Chapter 12- Other changes required by 5MLD

89 Are you content that the existing powers for FIUs and competent authorities to access information on owners of real estate satisfies the requirements in Article 32b of 4MLD as amended?

- We are satisfied that the use of existing data sources is sufficient to meet the requirements set out in the Directive for FIU's and competent authorities to access information on owners of real estate.

- Between the information available in the Land Registry, obtained through production orders and in government databases, there will be sufficient information on owners of real estate available. It should be acknowledged that such an approach would only be sufficient where the information requested and obtained from Estate Agents. is accurate and up to date. This should also give consideration to known issues within the Estate Agent sector in respect of robustness of due diligence measures.

- We note the approach to meeting this requirement for real estate owners, and stress that similar approaches of leveraging existing data sources should also be used to address other recommendations, such as those for the bank account register as per our response to Chapter 10.

90 Are you content that the government's existing approach to protecting whistle-blowers satisfies the requirements in Article 38 of 4MLD as amended?

- We are content that the existing requirements under the Employment Rights Act 1996 and the extension of these under Public Interest Disclosure Order 2014, meet the requirements of the Directive in ensuring whistle-blowers are legally protected from retaliatory or hostile action. In addition, we note that senior managers and certification regime includes additional whistle-blower requirements tailored to the regulated financial sector.

Chapter 13- Pooled client accounts

We welcome the addition of pooled client accounts to this consultation, and acknowledge the dedicated engagement between UK Finance and HMT, Scottish Government and the Ministry of Housing, Communities and Local Government over the last year. Progress in developing a workable solution to the issues around pooled client accounts is being made, in an effort to avoid the costs and complexities involved leading to the withdrawal of pooled client accounts as a service. We are pleased that following engagement with relevant stakeholders this draft proposal is near completion and ready to be submitted to the JMLSG editorial board for review.

91 Are there differences in the ML/TF risks posed by pooled client accounts held by different types of businesses?

The UK's 2017 National Risk Assessment of Money Laundering and Terrorist Financing reported:

- abuse of client accounts facilitated by complicit or negligent professionals is a key threat and vulnerability in relation to legal and accountancy service providers;
- UK law enforcement agencies have observed client accounts being exploited by criminals to transfer funds to third parties, effectively breaking the audit trail to launder funds;

- Additionally, the Solicitors Regulation Authority (SRA) has observed cases of solicitors not carrying out full due diligence on each transaction or facilitating client account transactions before the completion of CDD; and
- Criminals have entered apparently legitimate relationships with legal service providers, securing access to a client account, then changed their arrangements unexpectedly and with little explanation in order to pass funds to a third party.

There are two primary vectors of risk:

- the customer's clients abuse the Pooled Client Account without the knowledge of the customer; and
- The firm's customer is complicit in using the Pooled Client Account for money laundering or terrorist financing purposes, either willingly or under duress.

92 What are the practical difficulties banks and their customers face in implementing the current framework for pooled client accounts? Which obligations pose the most difficulties?

- It will be challenging for Financial Institutions to maintain the provision of pooled accounts for their customers who do not qualify for the simplified due diligence, SDD, exemption. This is due to the operational difficulties inherent in a relevant person identifying and verifying the identity of its customer's customers. Given the number of persons whose funds are held in a pooled account and the rapidity of changes to those persons, the Government should facilitate accelerated review and approval of suitable JMLSG guidance to ensure the SDD exemption is available for appropriate customers.

- Whilst letting and management agents are not noted as a high risk area within the NRA, there is a risk of significant customer disruption in the instance of a bank making a SAR in relation to its customer's pooled client account. For example, fungibility concerns leading to freezing the entire customer account to comply with POCA.

- This will have a significant impact on customers that rely on pooled accounts to operate, including those customers that are not relevant persons under the 4MLD / 2017 MLRs and therefore, by default, do not qualify for the Simplified Due Diligence exception (e.g. local authorities or letting agents).

- Banks that want to continue providing pooled accounts as a service must invest significant time and money in conducting enhanced due diligence (i.e. full CDD on its customer's

customers) on sectors not considered to be high enough risk to be subject to the 2017 MLR (e.g. letting agents), even though KYCC is not a legal requirement. In compliance with the risk based approach, this investment would be better directed to preventative measures associated with higher financial crime risk.

- The obligation to conduct CDD on the customer's own customer's is contrary to FATF's approach to correspondent banking, which similarly involves a customer that is subject to AML obligations providing services to their own underlying customers. In particular, a focus on nationals of high risk third countries will drive outcomes that are contrary to the Equality Act and will ultimately result in regulated firms withdrawing services from such nationals in view of the resultant legal risk.

- Where pooled accounts are maintained the impact on customers will be disproportionate; not only requiring governance arrangements to provide their Financial Institution with identification and verification details of their customers, but also repapering existing customer agreements / T&Cs to comply with GDPR. Importantly, customers that are not subject to 2017 MLRs will have to identify and verify their own customers to the standards of the 2017 MLRs.

- Where the customer is a relevant person under the 4MLD / 2017 MLRs but is not low risk, both the financial institution and their customer must identify and verify the owners of funds in the pooled account. This is an unnecessary duplication of effort and will, by adding another level of due diligence, act as a barrier to consumers' timely access to the services of solicitors, accounts, estate agents etc.

93 If the framework for pooled client accounts was extended to non-MLR regulated businesses, what CDD obligations should be undertaken by the bank?

- It would appear disproportionate for non-MLR regulated businesses, deemed too low risk to require regulation, to have CDD obligations more stringent than higher risk businesses that are regulated. Requiring FIs to apply additional requirements on unregulated firms could be perceived as "regulation by stealth." The likely impact of not de-scoping unregulated firms is therefore likely to be:
    - Significant cost impact on the unregulated firms;
    - Significant impact on firms that are outside of the regulatory framework but are considered high risk, the likely impact being an inability to open pooled client accounts; and

- A disproportionate increase in banks' cost to serve such customers, to the extent that banks will likely start to withdraw pooled client accounts as a service.

- UKF has been discussing this with a number of other professional associations, in both the regulated and unregulated sectors, and strongly encourage the Government to continue supporting a productive and proportionate approach.

- We would recommend that the CDD obligations for pooled client accounts for non-regulated sectors should follow the requirement for these business relationships to be low risk, but otherwise allow a SDD requirement. In practice, for typically low risk sectors this should allow a proportionate approach in the absence of any specific financial crime red flags.

Chapter 14: Additional technical requirements- Enforcement Powers

Enforcement Powers

94 Do you agree with our proposed changes to enforcement powers under regulations 25 & 60?

- We do not oppose the recommendation.

95. Do you agree with our proposed amendment to the definition of "officer"?

- There is no clear definition of manager across members different business models. Indeed, it is now common for staff of very junior levels to have job titles which include "manager" but who do not have the level of responsibility which we believe that it is intended that this apply to. Notwithstanding, we acknowledge the current definition contained within 2017 MLRs "means a person who has control, authority or responsibility for managing the business of that firm, and includes a nominated officer".

- There needs to be some consideration to how this definition applies for non-UK headquartered groups, e.g. would the definition apply globally.

- As HMT will be aware, the financial sector is already subject to the senior managers regime, which extends personal liability to senior managers within organisations. We recommend that HMT use the SMR regime criteria for the identification of individuals who should appropriately have personal accountability due to the materiality of their decision-making or management

oversight responsibilities. This would seem a more sensible approach than the the proposal put forward here.

- Equally, if the aim is to raise standards in other sectors this would be better done through an extension of the SMR to cover these additional sectors. It would be beneficial to understand exactly what this proposal is attempting to achieve. If the goal is, as mentioned above, to extend an equivalent of the SMR regime on “officers” of other sectors, we stress that the financial sector should be explicitly excluded from the change.

- As matters such as role, cross-jurisdictional groups and third country headquartered firms were all carefully considered and addressed in the SMR, we believe that the approach described above is best placed to deliver the intended result without any unforeseen or disproportionate consequences on the individuals in question.

Information Sharing

96 Do you agree with our proposed changes to information-sharing powers of regulations 51,52?

- We do not oppose the recommendation.

Requirement to cooperate

97 Do you have any views on this proposed new requirement to cooperate?

- We support this proposed requirement to cooperate.

Changes to the requirement to be registered

98 Do you agree with our proposed changes to regulations 56?

- We support the proposal to close the grace period for MSBs and Trust and Company Service Providers (TCSPs) which allows them to trade within the period before their registration application has been determined, considering the ML/TF risks associated within these sectors.

Complex network structures

99 Does your sector have networks of principals, agents and sub-agents?

- We do not believe that the banking and financial sector operates principal and agent structures within the context of this recommendation, which appears to be tailored to the structure of MSBs. This should be clarified for the avoidance of doubt. We believe this recommendation should be tailored to the MSB sector in order to address some of the concerns that are making this sector higher risk, and help to encourage banking of MSBs.

100 Do complex network structures result in those who deliver the business to customers not being subject to the training requirements under the MLRs?

- The answer to this question would be dependent on the proposed scope of this requirement.

101 Do complex network structures result in the principal only satisfying himself or herself about the fitness and propriety of the owners, officers and managers of his or her directly contracted agents, and not extending this to sub-agents delivering the business?

- The answer to this question would be dependent on the proposed scope of this requirement.

102 If you operate a network of agents, do you already provide the relevant training to employees? Do you ensure the agents who deliver the service of your regulated business are 'fit and proper'?

- No comment on this question.

103 What would be the costs and benefits to your business of the regulations clarifying intention to extend requirements to layers of agents and subagents?

- No comment on this question.

Criminality checks

104 Do the proposed requirements sufficiently mitigate the risk of criminals acting in regulated roles?

- We are supportive of the proposed changes in this proposal, although flag that considering existing requirements under Regulation 26, this information is likely already being provided.

New technologies (changes to regulation 19)

105 Should regulation 19(4)(c) be amended to explicitly require financial institutions to undertake risk assessments prior to the launch or use of new products, new business practices and delivery mechanisms? Would this change impose any additional burdens?

- Considering the current position within the 2017 MLRs and JMLSG guidance, many firms already conduct risk assessments before adopting new products and delivery mechanisms. We would stress however, that the terms “business practices” and “delivery mechanisms” would need to be clearly defined to ensure this requirement does not end up with a much broader scope than the anticipated focus on new technologies**.**

- We also note the importance of this requirement being aligned with recent European Banking Authority guidelines published on the adoption of new technologies given the increasing importance of new FinTech providers[9]**.**

Group policies (changes to regulation 20)

106 Should regulation 20(1)(b) be amended to specifically require relevant persons to have policies relating to the provision of customer, account and transaction information from branches and subsidiaries of financial groups? What additional benefits or costs would this entail?

- Existing policies and procedures will likely already address data protection and information sharing across a group. It is unclear exactly what this recommendation is referring to in terms of the specifics of the AML/CTF angle to these policies. Clarity is needed around the types of customer, account and transaction information that would be included within these policies.

- The impact will be significant if the requirement to have group wide policies and procedures for sharing customer, account and transaction information is considered to be in scope of Regulation 20(4). Most third countries currently allow sharing of risk information such as SARs or blacklisted customers as long as there are controls around tipping off. However, some of branches and subsidiaries operate in jurisdictions where they are prohibited from sharing customer, account or transaction information even with head office; others may be able to share information with head office but not other offshore branches/subsidiaries. There would be significant impact to branches and subsidiaries if additional measures are required where local laws prevent sharing of customer, account and transaction information.

[9] https://eba.europa.eu/-/eba-assesses-risks-and-opportunities-from-fintech-and-its-impact-on-incumbents-business-models

Annex A

Other Obliged entities - Telecommunication and Social Media Companies

As part of considering the specific questions posed in the Consultation, our members have identified two additional sectors, telecommunications and social media, which are not currently obliged entities but we consider users pose financial crime risks.

We believe that these sectors should also be considered, either as obliged entities or as otherwise incentivised to contribute to the UK's wider integrity and security regime. We have summarised below the elements of the existing framework which we consider to be relevant to these sectors.

A. General

- We believe that law enforcement should be able to give take-down or keep-open notices to social media and Telecoms companies, as they have in respect of transactions or bank accounts. We consider that the Government should takes the opportunity of new legislation to ensure that law enforcement have the powers they need to ensure all key sectors assist with law enforcement investigations and prosecutions.
- We consider that Ofcom's regulatory remit should be extended to include social media and internet service providers (ISPs) (as these are also communications channels). We also consider that their current consumer protection remit should be extended to incorporate financial crime prevention (we provide specific suggestions below of areas requiring regulatory attention).

B. Social media companies

- We consider that the use of social media companies, including ISPs, pose financial crime risks due to the multiple ways in which they are currently abused to enable and facilitate financial crime. For example:
    - Grooming for terrorism;
    - Advertising for money mules (commercially motivated);
    - Sales of stolen identity data and card data, including the prevalence of public sales sites on the Internet (as opposed to just the dark or deep web);
    - Inconsistent monitoring and identification of those at risk of grooming or performing lone wolf attacks to assist law enforcement with prevention measures, such as through relevant typology data and material changes in their search activity.

Regulated firms monitor for equivalent behavioural change in financial transactions, which can trigger red flags for SAR consideration;

C. Telecommunication companies (Telcos)

- We believe that if Telcos, including mobile telephone service providers, mobile telephone retailers and SIM retailers, pose high financial crime risks due to the multiple ways in which they are currently abused to enable and facilitate financial crime. For example:
    - Many criminals use techniques such as SIM swaps or number spoofing to circumvent the controls in place at financial services firms. For example, they will apply to a mobile telephone company for a duplicate SIM which will then enable them to circumvent the callback or text confirm procedures of banks for unusual transactions on their customers' accounts. The president of the Communications Fraud Control Association acknowledged following publication of its 2017 Global Fraud Loss Survey:
        - "*many services now utilise the mobile phone as the contact point for verification, whether this is to receive a call to verify a transaction or a text message with a one-time passcode or authorisation code. The mobile account of a consumer has become fundamental as part of an authentication trail in many services such as banking. Fraudsters therefore target customers accounts in order not to defraud the telecoms company but actually target the consumer themselves in order to manipulate their financial or other services*."[10]
    - Where multiple SIMs being used on the same device or from the same location, this can indicate organised crime SIM swap activity. It is not clear what controls Telcos have in place mitigate the risk of insider-fraud (e.g. in mobile stores where such SIMs etc. can be authorised for use by organised criminals, or the risk of call-centre staff being socially engineered to give such authorisations).
    - It is also not clear whether Telcos implementing new services or systems give explicit consideration of financial crime risk. For example, we are aware of continuing technical vulnerabilities of some mobile phones and some landlines to "keep line open" fraud attacks on their customers (e.g. where the criminal phones the customer with a scam designed to encourage them to phone their bank after the call and is then able to keep the line open so that they can hear the security answers provided by the customer when they do then phone their bank). We also consider that remote device

[10] https://www.thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807.

takeover is a continuing vulnerability (e.g. where organised criminals contact the customer and pretend to need access to the mobile device in order to run security checks on the device).

There are also inconsistencies in how Telcos take account of typology data provided to them by banks (e.g. where Telcos have been alerted by banks to the exploitation of vulnerabilities in their devices and specific cases of abuse by organised criminals to commit crimes in mainstream financial services). This inconsistency can lead to cases where such vulnerabilities have been left open to exploitation for material periods after the sharing of alerts.