Transposition of the Fifth Anti Money Laundering Directive

21 June 2019

By email to: Anti-MoneyLaunderingBranch@hmtreasury.gov.uk

1. The Association for Financial Markets in Europe (AFME) welcomes the opportunity to respond to the HM Treasury consultation on Transposition of the Fifth Anti-Money Laundering Directive. AFME represents a broad array of European and global participants in the wholesale financial markets. Its members comprise pan-EU and global banks as well as key regional banks, brokers, law firms, investors and other financial market participants. We advocate stable, competitive, sustainable European financial markets that support economic growth and benefit society.

2. AFME is the European member of the Global Financial Markets Association (GFMA) a global alliance with the Securities Industry and Financial Markets Association (SIFMA) in the US, and the Asia Securities Industry and Financial Markets Association (ASIFMA) in Asia. AFME is registered on the EU Transparency Register, registration number 65110063986-76.

3. In general, we find the proposals in the consultation to be a reasonable transposition of the Directive, but we would caution against too literal a use of wording which has been taken from the Directive and which does not sit well in a common law context. Paragraph 1.13 states that *"the government will only "gold-plate" (go further than) the provisions in 5MLD where there is good evidence that a material ML/TF risk exists that must be addressed*". Literal transposition from documents written for a civil law environment can have the effect of gold-plating, even if unintended, when used in a common law environment. This will lead in turn to the imposition of unnecessary additional procedures in a field of regulation which, as is generally agreed, is presently overburdened with procedures, an issue which does not assist its effectiveness as a whole.

4. There follow some specific points below, but our response should be read in the whole.

    - Cryptoassets: AFME recommends that HMT use the term "cryptoassets" rather than "virtual currencies" when transposing 5MLD into UK law. This recommendation is based on the definition of a "cryptoasset" as "a cryptographically secured digital representation of value or contractual rights that uses some type of distributed ledger technology and can be transferred, stored or traded electronically" by the UK Cryptoasset Taskforce[1] (see page 11 of their Final Report). Further, we request that HMT adheres to a clear and consistent taxonomy for the regulation of cryptoassets, and harmonises this taxonomy, wherever possible, with the work of other national, regional and global regulators in order to prevent regulatory arbitrage while developing an approach that fosters innovation.

    - Enhanced Due Diligence: 5MLD introduces a significant change to Article 18(a)(1) which expands its scope of persons on whom obliged entities must conduct EDD from 'natural persons or legal entities established in the third countries' to 'business relationships or transactions involving high-risk third countries'. The risks of business relationships and the risk of transactions involving high risk third countries are different. Hence, the EDD measures should be tailored to target the appropriate risk. We also encourage the government to ensure that clarity is provided as between direct and indirect high risk third country connections. The term 'involving' is capable of being too

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

broadly defined and for this reason can result in disproportionate application of EDD measures. In our response we seek to provide a very detailed understanding of the expressions 'involving, 'business relationship' and 'transaction' which we hope is helpful in shaping the government's views on how transposition of these EDD measures should be carried out with a view to ensuring that they are proportionate and effective in combating money laundering and terrorist financing.

- Obliged Entities: 5MLD suggests that whenever an obliged entity enters into a new business relationship with a company or trust that is subject to beneficial ownership registration requirement, they must (i.e. a mandatory requirement) collect either proof of registration on this register or an excerpt of the register. Our members believe that an obligation or obliged entities to check the register is understood, but there should be no obligation on obliged entities to verify the information contained in the register. Otherwise there is no point in having the register or the many third-party data providers who source information from it. It is the obligation of the government not of the private sector, to verify the data in the Companies Registry.

5. Our responses to individual questions follow. We have not answered every question but have rather picked out those of most interest to our members, whose businesses focus on the sell side wholesale capital markets. Thus, we have omitted answering the sections on expanding the definition of tax advisor, letting agents, art intermediaries, requirement to publish an annual report and certain other changes required by 5MLD.

Chapter 2 New Obliged Entities

Cryptoassets

General comments:

AFME welcomes HMT's efforts in bringing cryptoasset related activities under the scope of 5MLD. The risks associated with ML/TF are particularly relevant to cryptoassets, due to their truly global and digital nature, their ability to provide potential anonymity using digitised and decentralised networks and the continued inconsistency across jurisdictions regarding what is an appropriate regulatory and oversight regime. AFME believes there would be benefits to consumer protection, market integrity and financial stability if cryptoasset issuers, exchanges and custodians were required to develop cryptoasset related surveillance and monitoring systems for the reporting of suspicious transactions.

In summary,

- AFME recommends HMT consider how it would align the use of cryptoasset related terms and definitions to a common global cryptoasset taxonomy. A common global taxonomy would support consistency and alignment of the regulatory frameworks which are currently under consideration across multiple jurisdictions. This taxonomy should ultimately be underpinned by a common understanding of terms.

- Cryptoassets are digital and cross-border in nature, therefore AFME believes that a globally consistent regulatory framework is necessary to effectively reduce the risk of regulatory arbitrage and provide adequate consumer protection while developing an approach that fosters innovation. AFME recommends HMT to align its approach with the EBA's advice to the European Commission on cryptoassets[2] , in particular the sections on AML/CTF (see pages 20 - 21), which are also supported by ESMA's advice[3] to the European Commission (see section VII.9, page 36).

[2] https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf
[3] https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

- AFME recommends HMT to remain technology-neutral in its approach to cryptoassets to ensure the same activities are subject to the same regulation, irrespective of the way services are delivered. This is particularly important for the preservation of a level playing-field. However, AFME encourages HMT to also consider how technological enhancements may impact the risk profile and appropriate control frameworks required, or how firms may achieve regulatory compliance, where a flexible approach may allow for more efficient processes/systems to emerge.

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 [of virtual currencies] 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?

AFME believes all activities involving exchange, security and utility tokens should be captured for the purposes of the AML/CTF regulation. Indeed, this would ensure a level playing field is preserved, mitigate potential risks (e.g. consumer risks, market integrity risks and financial stability risks) and support greater market transparency and consumer protection across the cryptoasset market.

Under the FCA's recent Guidance on cryptoassets[4], the FCA suggests that "virtual currencies" fall under the category of "exchange tokens" only (see 3.31 page 21 of CP19/3), and AFME agrees with this definition. Therefore, AFME recommends HMT consider amending the term "virtual currencies" to "cryptoassets" in the application of the 5MLD to capture all types of cryptoassets (including virtual currencies). AFME recommends this using the UK Cryptoasset Taskforce's definition of "cryptoassets", being "a cryptographically secured digital representation of value or contractual rights that uses some type of distributed ledger technology and can be transferred, stored or traded electronically"[5] (see page 11 of their Final Report). This would ensure security tokens; utility tokens and exchange tokens are all captured under the 5MLD requirements.

We also believe this definition of cryptoassets incorporates other types of cryptoassets, which in our opinion, would not currently be captured by HMT's definitions of security, utility and exchange tokens. For instance, "stablecoins" as considered by the FCA[6] (see 3.65 page 31 in CP19/3) may be issued by clearly identified and regulated institutions and contain specific stabilisation characteristics which may cause them to fit imperfectly into one of the three previously identified token categories. In AFME's view, these stablecoins should be considered as cryptoassets and should be subject to AML/CTF regulation. For the purpose of providing additional clarity, AFME defines a "stablecoin" as a digital representation of a medium of exchange, a means of value transfer, a unit of account, and/ or a store of value using a digital platform, issued by a central issuer and thus redeemable, being partially or entirely backed by an underlying asset or asset basket.

Further, AFME is of the view that HMT's definitions of security, utility and exchange tokens may not cover cryptoassets which tokenise ownership rights for real assets such as art and real estate. We therefore recommend that HMT consider a taxonomy which includes other additional types of cryptoassets. We propose

[4] https://www.fca.org.uk/publication/consultation/cp19-03.pdf[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf
[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf
[6] https://www.fca.org.uk/publication/consultation/cp19-03.pdf

that a taxonomy for cryptoassets should be consistent across all institutions and jurisdictions in order to avoid unnecessary confusion and legal uncertainty for public and private sector actors, particularly within Europe.

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 5MLD definition [of custodian wallet provider] 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 the 5MLD definition, but should come within the UK's regime?

AFME broadly agrees with HMT's definition of a custodian wallet provider. However as per our response to question 12, we recommend HMT to amend the term "virtual currencies" to "cryptoassets" to encompass all relevant activity related to exchange, security and utility tokens and ensure alignment with the FCA's proposed definitions[7].

Therefore, 5MLD requirements for custodian wallet providers should apply to all those actors providing cryptoasset services (e.g. not simply for "virtual currencies") to ensure a level playing field across all market actors is maintained.

More broadly, AFME requests clarification in relation to pooled accounts: would a crypto wallet which is maintained by a custodian wallet provider, as defined above, become subject to client monies rules? If so, when and under what circumstances?

Furthermore, AFME recommends HMT consider how compliance with 5MLD requirements may be achieved differently in a digital and distributed environment, as technologies such as DLT may make it possible to achieve compliance more efficiently than when using current processes/systems.

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?

AFME believes that the FCA could indeed be the appropriate supervisory body for cryptoasset exchanges and custodian wallet providers, where appropriate.

However, AFME also recommends that HMT and the FCA consider how their efforts to encompass cryptoassets under their respective perimeters align with pan-European (European Commission, EBA, ESMA, ECB) and other Member States NCAs' activities, to ensure a coherent and consistent supervisory regime is developed across cryptoasset-related activity in Europe. There is a risk of market fragmentation if jurisdictions develop divergent approaches and supervisory practices for the regulation of cryptoassets, which could make more complex the fight against money laundering and terrorist financing

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?

AFME believes that without a globally consistent, common cryptoasset taxonomy and a globally consistent approach to the regulation of cryptoassets, there is a risk of regulatory arbitrage due to the global, digital and decentralised nature of cryptoassets.

[7] https://www.fca.org.uk/publication/consultation/cp19-03.pdf (see 2.3 – 2.5, pages 8 -9)

These risks were also identified by the ECB in its recent Occasional Paper on cryptoassets[8], where the ECB indicated that "at the time of writing, the legal status of crypto-assets varied among countries, absent a common taxonomy of crypto-assets, and a shared understanding of how crypto-assets should be treated from a regulatory standpoint. Given the global dimension of the crypto-assets phenomenon, uncoordinated and/or inconsistent regulatory approaches undertaken at the country level may prove ineffective and create incentives for regulatory arbitrage. Whilst this need not pose an immediate threat to the financial system, it calls for vigilance at the level of the EU, to prevent a proliferation of national initiatives from triggering regulatory arbitrage and, ultimately, hampering the resilience of the financial system to crypto-asset market-based shocks" (see page 28 of Paper Series No.223).

Similarly, without a globally consistent application of AML/CTF regulation to all types of cryptoasset providers, there is a risk of regulatory arbitrage and a non-level playing field, where those actors who are not required to implement AML/CTF requirements to the same extent as other jurisdictions will pose a risk to consumer protection, market integrity and financial stability, as well as to AML and CTF.

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.

AFME believes that the risks of ML/TF associated with crypto-to-crypto exchanges are equally as present as those risks associated with crypto-to-fiat exchanges. As such, to avoid additional potential ML/TF risks associated with the exchange of cryptoassets, AFME welcomes the requirement for all cryptoasset related exchange services to trigger AML/CTF obligations, including crypto-to-crypto transactions. This would ensure the entire value chain of cryptoasset related activity (e.g. end-to-end) is consistently captured under the same requirements, thus mitigating the risk of regulatory arbitrage.

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?*

As per our response to question 17, AFME believes AML/CTF obligations should apply to all cryptoasset exchange services (including peer-to-peer exchange services). This would ensure a consistent applicability of AML/CTF requirements across the cryptoasset value chain, as those actors could present a heightened risk for financial crime, if left unregulated.

Where those services (e.g. peer-to-peer exchanges) are conducted by firms who are regulated and authorised by the FCA, the regulation should apply consistently across all firms. Where those services are conducted by individuals, such as in-person exchanges or fully decentralised platforms, it may be more difficult to apply those regulatory requirements. In this instance, AFME supports the views developed by the ECB to use a principles-based approach that is complemented by a formal mechanism to validate the observance of such principles[9].

[8] ECB Occasional Paper Series No 223 / May 2019, p.29-30, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf
[9] ECB Occasional Paper Series No 223 / May 2019, p.29-30, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf

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?

AFME believes that the principle of technological neutrality should be maintained across all financial services regulation. With respect to open source software ("OSS"), it is important that HMT regulate not the technology, but the activities conducted using such technology, specifically how the software is used, and which proportionate controls are in place for ongoing monitoring and surveillance. As such, AFME cautions regulators against applying CDD checks to OSS. Further, there are no such CDD obligations for other financial software providers, and AFME believes OSS should not be treated any differently to independent software developers who are employed to produce solutions for other high-risk businesses such as defence, money services businesses, or on-line gambling. It would therefore not seem appropriate to apply these obligations to OSS providers.

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.

AFME supports HMT's proposal that firms involved in the issuance of new cryptoassets through Initial Coin Offerings should be required to fulfil AML/CTF obligations on their customers. In particular, where those ICOs are used to raise funds and involve marketing and sale of tokens, it is AFME's view that the issuer/seller should be required to undertake CDD checks.

AFME recommends HMT to consider the following:

- If the ICO is being undertaken directly by the firm, it should be the firm's responsibility to comply with client onboarding requirements. These should ensure that a similar (e.g. proportionate) level of diligence is conducted to that which would be undertaken in respect to the issuance of other traditional financial assets;

- if the firm involved in the issuance of new cryptoassets (e.g. ICOs) is using intermediaries, those obligations should also apply to those intermediaries; and

- if the issuance of new cryptoassets (e.g. ICOs) is undertaken on an exchange or platform, then the obligation should apply to that exchange or platform.

AFME believes the applicability of AML/CTF obligations to firms, intermediaries or exchanges, where relevant, is key to ensuring all parts of the cryptoasset value chain are consistently captured under the same requirements, in order to mitigate the risk of regulatory arbitrage which illicit actors may attempt to exploit.

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?

AFME strongly supports a globally consistent approach to the regulation of cryptoassets. It is AFME's view that only a globally coordinated approach would appropriately mitigate the risks of illicit activity and regulatory arbitrage. AFME encourages HMT to engage with pan-European (European Commission, EBA, ESMA, ECB) and global standard setting bodies (IOSCO, FSB, BIS, and the FATF) to promote and coordinate

the implementation of global approach to the regulation of cryptoassets, where a global common taxonomy would foster the common understanding of cryptoasset-related terms and definitions.

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?

AFME believes that certain cryptoassets are likely to hold more or less risk than others, based on their underlying risk profile, which would ultimately be underpinned by certain factors such as the issuer, the token's purpose, the underlying governance structure etc.

There is no clear definition of "privacy coins", however AFME understands that they could provide near total anonymity for their users, which would appear to imply significant ML/TF risk in some instances and could make CDD checks particularly difficult to conduct. Therefore, in light of HMT's proposal to require CDD checks for all exchange services, including crypto-to-crypto exchanges and all cryptoassets, AFME believes "privacy coins" would require particular consideration. However, without a comprehensive understanding of the risk profile of a particular "privacy coin", it would be difficult to make blanket statements on the risks and benefits of "privacy coins".

Regardless of the risk profile of "privacy coins", it should be the responsibility of the issuer or the platform (if traded on a secondary market), to comply with CDD requirements where those "privacy coins" would be issued or exchanged.

AFME believes that if regulated entities wish to engage in activities relating to "privacy coins", it should be the responsibility of the institution to ensure it is able to meet regulatory requirements from a CDD (and more broadly AML/CTF) perspective.

Chapter 3 Electronic Money

We note that under paragraph 3.5 of the consultation it is stated that "*5MLD 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 in 5MLD in relation to e-money."*

Can HMT please confirm that the term 'acquirer' is used in this context as it is defined in JMLSG part 2 paragraph 2.9 ''*Merchant Acquirers provide a payment card processing service, which facilitates acceptance of payment card transactions between cardholders and merchants'?*

Chapter 4 Customer Due Diligence

44, 45. 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? 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?

There is a need for principles-based guidance as to what constitutes "secure". However, the Joint Money Laundering Steering Group (JMLSG) Guidance, which is Treasury-approved guidance, and which is mentioned in paragraph 4.2 of the Consultation, exists to provide guidance to the financial services sector in interpreting

the MLR. It is not an appropriate forum for providing recognition (whether implicit or explicit), approval or acceptance of electronic identification processes. That is the role of national competent authorities.

The FCA Financial Crime Guide could, however, provide such recognition. Such recognition should include a statement that verification schemes in jurisdictions other than the UK will also be acceptable providing they meet the "secure" test.

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 other measures government could introduce to further encourage the use of electronic means of identification?

Historically governments have been unwilling to permit firms to rely on technological solutions and this will have to change. The more that government permits reliance by firms on technology the better. Implemented and governed appropriately across UK financial markets it would allow for quicker and more reliable identification, saving time and resourcing to focus on higher risk financial crime work. However, regulators must recognise that any new technology will always have teething problems, and so should be slow to enforce against obliged entities who genuinely are trying to improve systems or controls but in so doing may occasionally make mistakes.

Changes to Regulation 28

47, 48. To what extent 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? 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 paragraph 4.4 of the Consultation proposes that MLR Regulation 28 (3) should be amended to bring it in line with the FATF recommendations and more specifically the FATF standards ("Recommendation 10.9"). According to the Consultation, Recommendation 10.9 recommends that relevant persons be *required* (rather than take "reasonable measures") to determine and verify the law to which a body corporate is subject. There is no FATF Recommendation 10.9, so we suggest that, in fact, Criterion 10.9 of the FATF UK Mutual Evaluation Report is the correct reference here.

The FATF Recommendations do not, in fact, *require* the verification of a corporate client's constitution, the full name of all senior managers or the company's ownership structure in all cases. Rather, the Interpretative Note to Recommendation 10 provides (at paragraph 5(a) that a firm must identify the customer and verify its identity, and that the "*type of information that would <u>normally</u> be needed to perform this function*" (emphasis added) would be the name, legal form and proof of existence (which the Interpretative Note suggests could be verified by certain documentation) and, inter alia, "*the powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of relevant persons holding a senior management position…*" (as to which the Interpretative Note sets out no suggested verification steps).

We recognise that the FATF Mutual Evaluation Review ("MER") commented that there were "minor deficiencies" in the UK's implementation of CDD measures, stating that "*the requirement to understand a customer's ownership and control structure and business activity is not clear*" and "*the requirement to identify and verify the names of senior managers is not absolute (FIs are only required to take reasonable measures)*".

However, (a) the UK was nonetheless rated as largely compliant (b) the MER did not identify the absence of a mandatory requirement to verify a company's constitution as a deficiency in its conclusions, and (c) to the extent that the MER is read as suggesting that this is mandatory, it appears to cut across the language of the Recommendations themselves (which as noted above do not suggest there is an absolute obligation), and gold-plates the Directive.

The Interpretative Note also makes clear that the purpose of these steps is "*first, to prevent the unlawful use of legal persons and arrangements, by gaining a sufficient understanding of the customer to be able to properly assess the potential money laundering and terrorist financing risks and, second, to take appropriate steps to mitigate the risks.*"

"The Requirement to understand a customer's ownership…" remains in our view subjective and therefore a clearer sense of the UK's regulatory expectations and intended outcomes would be helpful. However specific CDD steps should not be introduced which gold-plate the FATF Recommendations and the Directive where these do not assist firms to understand or mitigate money laundering risk.

Proposed deletion of 'reasonable measures'

It is not clear what more can sensibly be expected of an obliged entity beyond taking reasonable measures. If the proposal is, in effect, a strict liability requirement to obtain verification documentation (for examples, for all members of management) in all cases then it conflicts with paragraph 1.13, which states that "*the government will only "gold-plate" (go further than) the provisions in 5MLD where there is good evidence that a material ML/TF risk exists that must be addressed*". Formalising a requirement always to determine and verify corporate information and details of large numbers of senior managers will create a burden on obliged entities far disproportionate to the risk that might be mitigated by obtaining such information. Similarly, verification of the law to which a body corporate is subject will not help address ML/TF risk.

Regulation 28(3)(b) already represents a key area where compliance requirements were introduced by 4MLD which serve little purpose in mitigating money laundering (for example, obtaining copies of Articles of Association for low risk corporate clients), and the removal of the "reasonable steps" test would eliminate what limited ability nonetheless remains for firms to adopt a risk-based approach.

In the case of verification of the identity of senior managing officials, we wonder in any event if this is not already covered by regulation 28(4)(b) of MLR17. It is already general practice to seek to identify at least one non-UBO senior manager.

Mandating "documentary evidence" is also inconsistent with the risk-based approach elsewhere permitted and also industry technological advances that enable electronic verification (such as that proposed for individuals).

Requirement to identify a senior manager as a UBO (where the 'true' UBO cannot be identified)

Paragraph 4.5 of the Consultation states that "*5MLD extends customer due diligence requirements for obliged entities to verify the identity of the senior managing official, when the customer is a body corporate and the beneficial owner cannot be identified."* Clarification of the meaning of the word "cannot" in this context would be helpful. We take this to apply, for example where our members have been unable to identify who the Ultimate Beneficial Owner (UBO) is, for example, due to non-cooperation by the client. Confusion may arise where our members have successfully satisfied themselves that a natural UBO does not exist. For example, for supranational organisations, multilateral FIs, government entities, sovereign wealth funds there would not

normally be an expectation that an individual beneficial owner would exist. For such client types, (e.g. the Reserve Bank of Australia, the United Nations) classification of a senior managing official as a "Beneficial Owner" could lead to a number of unintended consequences that simply add to the administrative burden with little obvious reduction in ML/TF risk, for example:

- Where the senior managing official is a Politically Exposed Person (PEP), mandatory application of EDD measures, which would run counter to the objectives of the PEP measures within the MLR; and
- Confusion at the client level where there will often be uncertainty or disagreement with the designated senior managing official not agreeing with the UBO designation leading to an unwillingness to provide verification documents and unnecessary strain being placed upon the client relationship.

AFME members therefore would appreciate specific guidance from HMT which clarifies the actual expectations of MLR Regulation 28(6), the previously requested clarification of the word "cannot", and the body corporates to which this requirement should be applied. We also seek HMT confirmation that the removal (if it transpires) of the term "reasonable measures" does not imply or mandate that firms must verify the identity of such individuals as if they were customers, nor to a standard that is more prescriptive/less risk-based than beneficial owners generally.

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?

Our members already generally gather this information, and support the idea that it should be an explicit CDD requirement, but subject to a risk-based approach which would permit lower or, as appropriate, higher levels of due diligence, for example such measures may be reduced where Simplified Due Diligence (SDD) is considered appropriate. The standard of "reasonable measures", which firms must currently apply in understanding the ownership and control structures of the corporate owners of customers (reg. 28(4)(c)) should be retained if the obligation is expressly extended to the ownership and control structure of customers.

Changes to Regulation 31

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 in the interests of clarity the requirements of regulation 31 should be extended to include the scenario where a firm cannot apply the required additional CDD measures (regulation 29).

In practice firms do consider, in all situations when CDD cannot be applied, whether there is a basis for suspicion, although the reasons for not continuing or completing CDD may not of themselves be suspicious, and may not trigger a SAR.

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

The two requirements should be kept separate. If a firm were to decide during EDD measures that a customer or transaction presented an unacceptable level of risk, a requirement to consider filing a SAR could be included. However, effectively lowering the threshold of suspicion for filing an SAR should be avoided as it will only result in an increase in the (already far too high) number of SARs that are filed but not acted on.

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

Extending regulation 31 to EDD measures to state that transactions should not continue without completion of EDD measures is unnecessary; however, there is potential for the EDD approval requirement to be met without completing other EDD requirements.

Chapter 5 Obliged entities: beneficial ownership requirements

Checking registers when entering into new business relationships

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)?

An obligation on obliged entities to check the register is understood, but there should be no obligation on obliged entities to verify the information contained in the register. Otherwise there is no point in having the register or the many third-party data providers who source information from it. It is the obligation of the government not of the private sector, to verify the data in the Companies Registry. See FATF Recommendations 24 and 25.

Also, will this work for trusts that have not yet been registered?

Requirement for ongoing CDD where there is a duty to review beneficial ownership information

54, 55. Do you have any views on the government's interpretation of the scope of "legal duty"? Do you have any comments regarding the envisaged approach in requiring ongoing CDD?

Paragraph 5.10 appears to be suggesting a box-ticking approach (in the two bullet points) as being obligatory above and beyond normal risk based periodic review timelines that are already in place within our member firms. We would oppose this, as both unnecessary and as contradictory to a risk-based approach. This new idea, if implemented, would significantly and disproportionately increase normal CDD requirements

We would encourage HMT to clarify what "legal duty" means. We are not sure how this new requirement for ongoing CDD where there is a duty to review beneficial ownership and relevant to ML/TF information would apply in practice. One possibility would be to focus on the requirement in regulation 27(9)(a), which is to the effect that one of the relevant risk factors which may require CDD measures to be performed in respect of existing customers is an indication that the beneficial ownership of the customer has changed. Another important issue is the nature and extent of CDD measures that must be performed when there is a relevant triggering event.

In any event a narrower definition of "legal duty" which focuses solely on CDD information relating to beneficial ownership would be preferable. Various factors are considered in a customer risk assessment, and these may not necessitate reconfirming beneficial ownership. A full review/update of the CDD file should not be required unless necessary to mitigate additional risk.

Chapter 6 Enhanced due diligence

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

The risk of business relationships and the risk of transactions involving high risk third countries are different. Hence, the EDD measures should be tailored to target the appropriate risk. For example, conducting enhanced monitoring and understanding the nature/purpose of the transaction may be sufficient to mitigate the risk from transactions involving high risk third countries instead of requiring all the EDD measures in 6.5-6.8 of the consultation.

The government should further ensure that clarity is provided as between direct and indirect high risk third country connections. The term 'involving' could be broadly interpreted to include relationships where the customer has some activity or revenue derived from a high risk third country. This would be disproportionate. We would suggest that the meaning of "involving" in the context of a "business relationship" be restricted to mean dealing with entities incorporated in or having their principal place of business in high risk third countries.

A more expansive interpretation would mean, by way of example, that the Red Cross would be subject to EDD measures and firms would be discouraged from dealing with charities that operate across borders including in high risk third countries. This would run contrary to FATF Guidance on Non-Profit Organisations.

5MLD aligns with FATF Recommendation 19 by mandating EDD measures not just on 'business relationships' involving high risk third countries but also on 'transactions'. 5MLD does not, however, define 'transactions'. Our view is that the term 'transactions' in the context of article 18a does not introduce a new situation where relevant persons must conduct due diligence. Instead, article 18a simply means that where a relevant person already has an existing obligation to conduct due diligence (i.e. under regs 4 and 27 of the MLR2017) and the customer 'involves' a high risk third country, then the relevant persons must apply relevant mandatory EDD measures if the involvement of the high risk third country gives rise to a higher ML/TF risk.

The reasoning is as follows:

- FATF 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). It specifies that they must also comply with the CDD requirements of Recommendation 10 (i.e. they must conduct CDD when establishing a business relationship or carrying out an occasional transaction), where there is suspicion of ML/TF, or where the firm has doubt about the veracity or adequacy of previously obtained customer identification data.

- 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 Recommendations 10 and 22 (i.e. when FIs and DNFBPs already have

to conduct due diligence). Recommendation also makes clear that the type of EDD measures should be 'effective and proportionate to the risks'.

- Article 18a of the 5MLD transposes (copies) FATF Recommendation 19. The term *'transaction'* in article 18a therefore simply refers back to when relevant persons already have to conduct due diligence. For AFME members (as well as DNFBPs) this means due diligence on business relationships and occasional transactions as per regulations 4 and 27 of the MLR2017. Recital 12 of 5MLD also makes clear that EDD should be directed at managing and mitigating risk posed by high risk third countries.

The proposed exemption for UK nationals is welcome but should be extended to all EEA nationals and nationals of other lower risk jurisdictions such as the US, Canada, Hong Kong SAR, Singapore, Australia or the like.

For those of our members who have offices in high risk third countries it is not feasible to require full EDD for all domestic business relationships or transactions. Strict enforcement of this rule could result in these offices closing, and would effectively be a regulator-inspired de-risking exercise, which is in no-one's interests, and certainly not helpful in the fight against money laundering and terrorist financing.

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 agree, but would seek clarification that Bancassurance relationships (a bank acting as an intermediary to offer insurance products from other providers to the bank's clients) would not be in scope.

Clarity on risk factors is always welcome provided it is consulted on in advance and not imposed unilaterally by regulators (whether in the form of new regulation, guidance, Q&As, Dear CEO letters, speeches or other means).

There is a further change introduced by 5MLD which is not discussed in the consultation, but which is potentially significant. Regulation 33 currently requires EDD to be conducted in any case where a transaction is complex and unusually large, or there is an unusual pattern of transactions *and* the transaction(s) have no apparent economic or legal purpose. 5MLD amends Article 18 to require EDD when a transaction is complex, unusually large, concluded in an unusual pattern, or does not have an apparent economic or lawful purpose. By their nature, many of the transactions undertaken by AFME members will be "complex" (and may be large in absolute terms) but may present a low ML/TF risk. The transposition of this amendment requires careful consideration so as to avoid unintended impacts; it will be important to retain the concept of a transaction being unusually complex (i.e. complex compared to what would be expected for a transaction of that type or for that customer), rather than introducing mandatory EDD in respect of all transactions that can be viewed as "complex".

Chapter 7 Politically exposed persons: prominent public functions

59. Do you agree that the UK functions identified in the FCA's existing guidance on PEPs, and restated [at paragraph 7.7], are the UK functions that should be treated as prominent public functions?

Yes, subject to the comments below, but senior positions within devolved regional or local government should be added.

We also note that the 5MLD obligation is to specify the "*exact functions*" which qualify as prominent public functions, under national law, regulations and administrative positions. The proposed list contains a number of elements of inexactitude. For example, it is said that in relation to ambassadors etc "*it will not normally be necessary to treat public servants below Permanent or Deputy Permanent Secretary*". What is the 'abnormal' case when other ranks are in scope, and which specific ranks are those (and why has the "*not normally*" qualifier been added, when it does not appear in the FCA guide)? Members of the national governing bodies of political parties should only be treated as exercising a prominent public function "*where they exercise significant power (e.g. over the selection of candidates or the distribution of significant party funds)*". We note that the "*e.g.*" signifies that these are non-exhaustive examples. We would like to know what other roles should be regarded as "*exercising significant power*"?

In relation to for-profit enterprises in which the state has an ownership interest of 50% or more "*or where reasonably available information points to the state having control*", we would like to understand why is it left to individual firms to seek to assess whether any particular entity, based on public domain information, is state-controlled, when we believe this could simply be specified by the state?

As such, the FCA's guidance provides a helpful base for a list, but greater specificity is required in order to discharge the requirements of 5MLD.

We would also suggest that this list be extended to cover all (non-EU) countries (on the assumption that the Commission will publish the lists prepared by other EU member states). There seems to be no logical reason for the UK to be treated as a special case. Laundering in the UK of proceeds of corruption from overseas is clearly a material ML risk.

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, provided the government is clear about which such UK-headquartered intergovernmental organisations will be in scope.

Chapter 8 Mechanisms to report discrepancies in beneficial ownership function

61, 62, 63. Do you have any views on the proposal to require obliged entities / competent authorities to directly inform Companies House of any discrepancies between the beneficial ownership information they hold, and information on the public register at Companies House? 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?

There is a need for a single approach when it comes to development of the Companies House registry. Therefore, a comprehensive joined up UK strategy is required.

We would also greatly welcome improved data in the Companies House registry, and note that the Department for Business, Energy and Industrial Strategy launched a consultation on the subject on 5 May 2019, which we are currently considering.

For the purposes of this consultation on 5MLD however, and without prejudice to any points we may make in our response to the DBEIS consultation, our initial thoughts are that Companies House, acting together with competent authorities, is best placed to identify fraudulent entries in its register. There would be a substantial

additional burden placed on the private sector by the proposal for obliged entities to assist the public sector to resolve its problem.

The proposal also appears inconsistent with FATF Recommendations 24 and 25, which instead places the obligations on the government in the first instance, as a means of supporting and enabling the CDD obligations to be undertaken by the private sector. Currently firms source their information from third party databases which in turn rely on public sector registries such as Companies House, so it is not clear that false data would in fact easily be picked up by this proposal. It might be easier and more effective for competent authorities to liaise directly with Companies House.

A further problem is that that the definitions of a Person of Significant Control (PSC) for the purposes of the registry and a UBO for the purposes of the MLR are not the same. They will in most cases yield the same result, but not always, and there are scenarios in which a firm might identify a "discrepancy" between the register and the CDD information it collects, simply because the applicable tests are different, and where the PSC register is in fact correct.

If these proposals were implemented, some sort of efficient feedback loop would be essential. Without a feedback mechanism, clarification of the client information (both beneficial ownership, and broader) will be sought by both the public and private sector. Resolution of reported discrepancies would involve investigation and cooperation from the impacted parties, which might well have tipping off implications, and resourcing implications for Companies House (who would need to review/resolve the discrepancies before posting the proposed public warning).

While no doubt this idea might assist in improving the quality of the data it is unlikely to solve the root cause of the problem, which is false information being fed into Companies House and not adequately checked there.

Legal protection for firms reporting discrepancies (from potential tipping off liability, breach of confidentiality, and from any loss which might flow from the company being reported) would be also essential.

Chapter 9 Trust Registration Service

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.

The scope appears very broad. It will be necessary for the government to put in place measures to ensure that trustees are aware of their obligations.

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 suggest that, in reality, the onus will fall on obliged entities to notify trustees of their requirements and explain what they mean which will lead to material delays in the on-boarding process.

We note that when entering into a business relationship with an in-scope trust, firms need to obtain proof of the registration with HMRC. In practice we expect firms will not want to provide financial services until registration is completed, however we would like to know whether on-boarding an in-scope trust will be

restricted without prior registration. Depending on the implementation approach, there may be a backlog of the ability to register, thus compounding delays even further.

Harmonisation with EU member states is important in relation to interpretations of what types of trusts must register, and what information must be collected.

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

Setting an element of duration at 12 months may be difficult to assess at the beginning of a business relationship and may result in all trusts registering even where it is not clear if the business has an element of duration. How 'working interactions' are defined is also unclear. Working interactions suggest an element of instruction and this may not include, for example, incoming payments.

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.

The purpose of the trust may assist as it could potentially allow detection capability between what financial institutions are advised is the reason for the business relationship and purpose of the trust, and what has been registered as the purpose.

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.

There will be additional costs and resourcing impacts, as Trustees will now have to complete two parallel almost identical verification requirements across both public and private sectors.

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?

This information is more stringent than that required in all cases by the private sector for CDD purposes, following a risk-based approach. Whilst this information can be helpful to identify common roles undertaken by the same individual across multiple trusts and for cross-border CDD where obtaining this information is a requirement in other countries, our members' experience is that individuals may be reluctant to share national ID number information.

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 cannot comment on the impact on trustees or agents. The impact on obliged entities, however, will be considerable, due to conflicting timelines for the requirements. We suggest the effective dates should be aligned.

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.

This will depend on the effectiveness and user-friendliness of the TRS systems.

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.

A utility model would seem the most appropriate, building in a "consent to share data" button for trustees to authorise specific persons to see their data.

Alternatively, UK FIs could be granted open access to the registry without having to demonstrate a "legitimate interest". This would assist FIs in meeting the proposed obligation to confirm trusts are registered as part of the onboarding process (if this becomes mandatory) however we do note that access to the TRS will not materially assist obliged entities with their CDD obligations, unless they are permitted to rely on it for CDD purposes (see also answer 46).

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.

Self-declaration is less resource-intensive than other methodologies, but is self-evidently open to abuse by the minority of trusts that will have been set up for ML purposes.

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.

Sharing data is in itself a positive idea. However, access to the TRS will not materially assist obliged entities with their CDD obligations, unless they are permitted to rely on it for CDD purposes (see also answer 46).

Chapter 10 National Register of bank account ownership

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

Per the MLR, firms are not required to collect unique identification numbers for related parties, such as signatories or beneficial owners, so the proposal represents a material back-door change to regulation 28, which should be the base line (but firms should be able to provide more data if they so wish). This information is not available in data providers or in the public domain. Again, a utility model would appear appropriate to avoid unnecessary duplication and technology/development costs.

Further, the exact requirements remain unclear. Is the intention for all accounts to be included in the central bank account register regardless of the entity type (institutional clients) or structure? We would recommend to target the scope of accounts to those which are of primary risk concern.

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?

Depending on the scope of the accounts envisaged for the national register of bank account ownership, in the institutional context the party which is subject to CDD may not be the same party that has the assets in the account e.g. segregated accounts for sub-custody business; funds and fund managers. Firms would not have a CDD obligation for segregated account holders and may not have a CDD obligation in relation to funds managed by an Investment Manager.

It needs to be clear that there is no requirement to verify ID numbers, as this would represent a material regression of the risk-based CDD regime in the UK. Given the amount of remediation that would be necessary if obtaining and/or verifying ID numbers is now mandatory, the system design needs to take this into account as most firms will not have such data on file. Firms need clarity on the degree of complexity of data requested as it will materially affect the cost of system and process development.

Chapter 13 Pooled client accounts

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?

The ESA guidelines do not mandate firms to conduct CDD on the underlying clients. Rather they require that the underlying clients be identified and verified as "beneficial owners" of the account.

It is challenging to determine the "beneficial owner" of the underlying funds since the composition of funds in a PCA is very fluid – it changes, for example, every time a transaction is completed.

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

Firms should apply their own judgment to assess the risks of the client and their underlying customers; including their non-regulated status, the extent of any due diligence undertaken. This should not be prescriptive; the onus should be on firms to develop their own risk assessments (baselined against the risk factors in MLR) and be able to justify their risk assessment and corresponding due diligence. This risk assessment may inform the nature and extent of CDD measures applied.

If the ownership of the economic interests of the account is widely dispersed, there should be no requirement to ID&V each individual interest holder as the volume may be disproportionate to the risk; subject to frequent changes; would be inconsistent with the approach taken in comparable areas, such as segregated accounts in the institutional custody context (e.g. the FATF RBA Guidance on the securities sector) and due diligence on collective investment vehicles, such as funds).

Chapter 14 Additional technical amendments to the MLRs

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

We suggest you restrict enforcement action to senior managers (and potentially certified persons) so as to avoid creating yet another, different and overlapping set of individuals who may be enforced against.

104. 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?

No. This runs counter to the risk-based approach. The JMLSG (chapter 4.23) uses the wording "*such a risk assessment should take place prior to the launch…"* which we take to be non-mandatory and AFME believes this is the correct approach.

105. 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?

We do not support this amendment. It should be left to each relevant person to decide whether or not to have such policies as part of its group-wide programme.

AFME Contacts

Will Dennis
Will.Dennis@afme.eu
+44 (0)20 3828 2683

Aleksandra (Ola) Wojcik
Aleksandra.Wojcik@afme.eu
+44 (0)20 3828 2734

Emmanuel Le Marois
Emmanuel.LeMarois@afme.eu
+44 (0)20 3828 2674

Madeline Taylor
Madeline.Taylor@afme.eu
+44 (0)20 3828 2688