Response to HMT Consultation on the Transposition of the Fourth Money Laundering Directive

Introduction

The Association for Financial Markets ("AFME") welcomes the opportunity to comment on Her Majesty's Treasury's Consultation (the "Consultation") on the Transposition of the Fourth Money Laundering Directive ("4AMLD"). AFME is a trade association representing the interests of European wholesale markets. Our members include the leading global and European banks as well as other significant capital markets players. 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 listed on the EU Register of Interest Representatives, registration number 65110063986-76.

We summarise below our general comments on the consultation, which is followed by answers to some of the individual questions raised. Where we have not answered any given individual question, AFME as a trade association does not have any specific views thereon.

General comments

AFME supports the efforts of legislators and regulators of the world over to combat money laundering and terrorist financing, AFME's members are committed to this. Money laundering provisions and procedures do need however to follow a risk based approach. Too much prescription is not helpful. Banks need the flexibility to be able to devise their own due diligence processes which, of course, will be subject to challenge by regulators.

Harmonisation of AML and CTF rules across national boundaries is also important, leading to greater mutual understanding of the rules as well as to simplicity of process. The use of new technologies such as KYC databases will assist regulators and banks alike, but is unlikely to come to pass if different jurisdictions continue to produce different rules. It follows that we are in general opposed to any gold plating of 4AMLD.

We note that HMT has not consulted on the proposals put forward by the European Commission in July 2016 to add provisions to the previously-agreed text of 4AMLD and to bring forward its implementation to 1 January 2017. We will be commenting separately on these new proposals, and will respond to any HMT or other consultation paper that addresses them. For now, we restrict our comments thereon to the statement that we believe it to be unrealistic for banks, and indeed for regulators, to be able to implement these new proposals by July 2017, let alone January.

Finally, it should be noted that the General Data Protection Regulation ("GDPR") will be enforceable within the EU from 25 May 2018. Given that firms can be fined up to €20 million or 4% of their total world-wide turnover for GDPR breaches and given also the capacity of the GDPR to restrict preventative AML/CTF activities under 4 MLD and more generally, it is important that implementation of 4 MLD is undertaken in a way that aligns with the GDPR. We have highlighted how this can be achieved in our response below.

afme/
Finance for Europe

Responses to individual questions

Question 3: When do you think CDD measures should apply to existing customers while using a risk-based approach?

AFME believes CDD measures should in general apply to existing customers, with the extent and timing of this determined through the application of a risk based approach. There should be no one-size-fits-all or over-prescriptive approach.

Question 4: What changes to circumstances do you think should warrant obliged entities applying CDD measures to their existing customers? E.g. name, address, vocation, marital status etc.

AFME believes that it should be left to individual firms to determine, on the basis of their risk-based bespoke internal policies, the exact changes in circumstances that warrant the application of CDD measures to existing customers. There should be no one-size-fits-all or over-prescriptive approach.

Question 7: Do you agree that the government should remove the list of products subject to SDD as currently set out in Article 13 of the Money Laundering Regulations (2007)? If not, which products would you include in the list? Please provide credible, cogent and open source evidence to support inclusion. What are the advantages and disadvantages of retaining this list?

AFME is not averse to the removal of the list of products only, as listed in Article 13(7) of the Money Laundering Regulations 2007.

Question 13: Are there any other products, factors and types of evidence of potentially higher risk situations, aside from those listed in Annex III of the directive, which you think should be considered when assessing ML/TF risks in respect of EDD? Please support your response with credible, cogent and open-source evidence where possible.

Further guidance on higher risk products would be helpful. This should however be drafted on the basis of principles, with firms left to undertake their own due diligence on the basis of a risk based approach bespoke to each firm. Additional guidance should not constitute a prescriptive minimum. So long as firms adequately document their decisions, they should be given the flexibility to explain why, in the light of their own circumstances, they feel that EDD is not necessary.

AFME would also appreciate further alignment of any additional guidance with FCA outputs including, but not limited to, those arising out of the FCA's Systematic Anti-Money Laundering Programme.

Question 15: What EDD measures do you currently apply to clients operating in high-risk third countries, including those on FATF's black, dark grey and grey lists?

This question is unclear, as the term 'operating in' is not defined. AFME member firms tend to apply a range of measures to clients established in high risk countries. These vary according to the perceived risks our member firms assign to such clients; and may include checks on such clients' customers, residency, beneficial ownership, types of products and services offered, subsidiaries and parents with links to high risk third countries, source of funds, source of wealth and any ongoing investigations. They may also include requirements for senior management approval as well as restrictions on the products and services that will be supplied to such clients.

Question 19: If you are a financial institution, are there any additional institutions or persons situated in a Member State or third country that you think could be relied upon in order to help reduce the regulatory burden on businesses - e.g. the third party applies due diligence and record-keeping requirements and are also appropriately supervised in accordance with the directive?

Under existing regulatory practice, it is unsafe for banks to rely without checking upon data supplied by third parties, whether in EU member states or in third countries, and whether or not the third party is a member of the same banking group to meet CDD requirements.

AFME however believes that this is an area in which there is room for the application of a risk-based approach which would enable third party KYC databases and/or other technology to make data available to banks which banks do not directly source themselves, with a view to permitting them to rely on this data.

Question 48: What impact will implementing the new definition of correspondent banking have on your firm's policies and procedures?

AFME Members are concerned that the new definition within the Directive appears to imply that the accounts between financial institutions used for securities settlements, either on behalf of themselves or their clients, can be used to transmit funds (whether or not the proceeds of crime) around the world, just like conventional correspondent banking accounts. The suggestion within the Consultation Paper is that these transactions would also be subject to EDD. It is however noteworthy that the Commission in its original impact assessment published in February 2013 failed to identify any such problem. As such, given the limited risks in such instances, AFME believes that a requirement for EDD in such circumstances would entail disproportionate costs and deployment of resources whilst also being impractical to implement.

Question 52: The directive specifically applies to members of parliament or of similar legislative bodies and to members of the governing bodies of political parties. In the UK the Electoral Commission maintains two registers of political parties: one for Great Britain and a separate register for Northern Ireland. There are over 400 registered political parties, of which the vast majority are very small. Should there be some form of criteria or some examples set out in guidance of the political parties to which this applies, e.g. those having elected members of Parliament, the European Parliament, or the devolved legislatures? If so, what is the reasoning behind the use of these particular criteria or examples? Would guidance on this issue assist and, if so, what should the guidance include to provide clarity?

We suggest that EDD should be limited only (whether in the UK or elsewhere) to serving members of the relevant parliament and those political parties that have access to public funds. The alternative would be impractical and disproportionate.

Question 59: How would you define an international sporting federation?

AFME believes it would not be appropriate to define all persons associated with international sporting federations, whatever that term may mean, as PEPs. Some sporting governing bodies may well, of course, include PEPs on their boards or in their governance framework.

Question 67: The government would welcome your views on retaining documents necessary for the prevention of ML/TF for the additional 5 years. What do you think the advantages and disadvantages are of doing so?

The main disadvantage of this proposal is that it could potentially give rise to a legal challenge either under the GDPR (Article 17 – right of erasure) or under the Charter of Fundamental Rights (Article 7

respect for private life and Article 8 right to protection of personal data). Any legal challenge to firms on account of their AML/CT deterrence activities would entail some legal costs for them, however a successful legal challenge under the first of these provisions could result in the application of significant fines to our Member Firms under the GDPR once it is in force.[1] Indeed in this respect, it should be noted that the EU data protection advisory body, the Article 29 Working Party, was highly critical of the document retention periods envisaged by 4 MLD.[2]

Question 73: Do you agree with the government's approach to a "person who holds a management function" in paragraph 12.13 - namely those who make decisions about a significant part of the entity's activities or the actual managing or organising of a significant part of those activities? Do you think it will encompass all individuals that should be subject to a fit and proper test?

Although the Senior Managers and Certification Regime (SMCR) has not yet been extended to all FSMA authorised firms, AFME believes that when this is done there may be merit in aligning the approach of "management function" in paragraph 12.13 to "senior management function" under the SMCR.

Question 74: Should the government extend the fit and proper test to agents of MSB's? Please explain your response and provide credible, cogent and open-source evidence where possible.

Subject to the principle of proportionality, yes.

Question 87: Do you have any further views not specifically requested through a question in this consultation that would help the UK provide effective protection for the financial system? Please provide credible, cogent and open-source evidence to support your views, where appropriate.

Yes. Please see below.

The GDPR will be enforceable within the EU with effect from 25 May 2018. It will both limit the circumstances in which data can be processed and will introduce more extensive penalties for breaches of its provisions, with the effect that firms can be fined up to €20 million or 4% of their total world-wide turnover for GDPR breaches. In the light of this, and the risk of conflicts between the GDPR and 4 MLD in the event that they are not implemented in a way in which they align with each other, we believe that it is imperative that a joined-up approach to implementation of 4 MLD is adopted. Specifically, this should take into account relevant provisions within the GDPR and involve close liaison between the HMT and the Department of Culture, Media and Sport.

In relation to the GDPR itself, we have highlighted some key issues that warrant further consideration below in the context of transposition of 4 MLD and ultimately implementation of GDPR. In the event that further detail is required, we would be happy to provide our more detailed analysis paper on request.

a. Grounds for data processing

With effect from May 2018, all data processing must be underpinned by a legal basis within the GDPR. Article 6(e) of the GDPR permits processing of personal data where it is in the 'public interest'.[3] We note

[1] This enters into force on 25.05.18 and firms can be fined up to €20 million or 4% of their total world-wide turnover for GDPR breaches

[2] Article 29 Working Party Correspondence, 8 November 2013 referring to its Recommendations, at p.23, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en_annex.pdf

[3] This must be 'laid down' by EU or Member State law

that by Article 43 of 4 MLD the 'processing of personal data on the basis of [The Directive] for the purposes of the prevention of money laundering and terrorist financing…shall be considered to be a matter of public interest under *Directive 95/46/EC*.' Article 94 of the GDPR requires that references to Directive 95/46/EC shall be construed as references to the GDPR and as such, going forward, it is important that 4 MLD implementation adequately reflects this.[4]

Furthermore, Article 9 of the GDPR prohibits the processing of 'special categories of personal data' such as political opinions and racial and ethnic origin. AML processing may require the processing of such data. For example, data relating to PEPs may imply political opinions and data relating to ethnicity and race could be involved when checking a customer's passport for identity verification purposes. Exceptions to this prohibition are listed in Article 9(2) of the GDPR. Article 9(2) refers to processing that is necessary for reasons of 'substantial public interest', as set out in EU or Member State law. In the light of Article 43 of 4MLD, it would therefore be helpful for implementing legislation to confirm that data processing undertaken to prevent money laundering or terrorist financing will be treated as processing that is undertaken for reasons of '*substantial* public interest'.

Finally, under the GDPR, the processing of 'personal data relating to criminal convictions and offences or related security measures', as per Article 10 of the GDPR, is permissible only in circumstances where

this is authorised by Union or Member State law. Therefore, appropriate implementing legislation will be required to ensure that such processing, in the context of anti-money laundering and terrorist financing activities/initiatives, can continue to be undertaken.

It is worth noting that the above *general points* are also relevant to deterring other forms of financial crime such as tax evasion, bribery and corruption, cyber-crime and fraud.

b. Data subjects' rights

Articles 12-22 of the GDPR set out a range of rights for data subjects. In the absence implementing legislation that makes use of the relevant GDPR exemptions to these rights, activation of these rights could impair attempts by banks to combat money laundering and terrorist financing. We have highlighted below the key rights of concern to us together with the exemptions that could be activated to address these.

- **Data subjects' rights to information** - Article 14 of the GDPR requires firms to provide extensive information to data subjects about data processing, including about the source of data where this has not been obtained directly from the data subject. Making available this level of information to data subjects could put AML CTF investigations at risk. Article 14(5)(c) provides an exemption where '…obtaining or disclosure is expressly laid down by Union or Member State law…' Articles 39(1) [5] and 41(4) of 4 MLD restrict the rights of data subjects to access data where the firm is meeting its 4 MLD obligations and to prevent official/legal investigations, analysis, etc., from being jeopardised

[4] Whilst other grounds for data processing exist, firms cannot safely rely on these for AML/financial crime processing. For example, data subject consent as per GDPR Article 6(1)(a) can be withdrawn at any time, which makes it unusable in this context. Further, in relation to complying with 'legal obligations' as per Article 6(1)(c), a significant amount of financial crime data processing is not, for the purposes of the GDPR, undertaken on the basis of 'legal obligations' but instead on the basis of FCA regulation and high level principles, JMLSG guidelines, FATF standards and thematic findings by the FCA, etc. Similarly, although firms could rely on their 'legitimate interests', as per Article 6(1)(f), as a basis for processing, this would leave firms in a vulnerable position given data subjects' enhanced rights under GDPR, covered below.

[5] It should be noted that similar exemptions are provided for under Part IV of the Data Protection Act, and these proposals amount to ensuring that these keep pace with changes under 4 MLD and the GDPR.

- **Right to erasure of data** – Article 17 of the GDPR creates the right to have one's data erased but sets out in Article 17(3)(b) specified exceptions to this right in circumstances where erasure would impede data controllers performing tasks in the 'public interest'

- **Right to restrict processing** – Article 18 of the GDPR enables data subjects to restrict processing in certain circumstances. Article 18(2) sets out exceptions to this including for 'reasons of important public interest of the Union or a Member State'

- **Right to object to processing -** under Article 21 GDPR data subjects have a right to object to (and therefore block) data processing except where there are 'compelling legitimate grounds' for this processing to continue

- **Profiling** – 4 MLD sets out requirements for the application of CDD and other processing activities that can be undertaken with varying degrees of automation. Article 22 of the GDPR however creates a right for data subjects 'not to be subject to decisions solely based on automated processing, including profiling in circumstances where this produces legal effects/significantly affects' data subjects. By Article 22(2)(b) an exception is created to this right where this is expressly authorised by Union or Member State law and meets further requirements within that provision

In order to address these issues, we recommend that MLD 4 implementing legislation clearly states that:

- There is an exemption from access rights where this would jeopardise AML or CFT processing
- Processing for the purposes of AML or CFT is to be considered both a 'substantial public interest' and also an 'important public interest' for GDPR purposes
- AML CTF processing constitutes a 'compelling legitimate ground' for continuing processing
- Automated decision making for AML CTF purposes is authorized under UK law

Where any gaps exist, Article 23 (1) of the GDPR provides an alternative means to ensure that there are appropriate AML/CTF exemptions from the GDPR. By Article 23, Member States are expressly empowered to restrict the application of those rights appearing in Articles 12-22 on specified grounds.

Key permissible grounds for restrictions are set out in Article 23(1)(d) of the GDPR. This refers to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. They are also set out in Article 23(e) of the GDPR. Article 23(e) refers to 'other important objectives of public interest of the Union or of a Member State'.

Additionally, as our Member Firms include multinational members who are subject to AML & CTF obligations that derive from 3rd countries, it is important for 4 MLD implementing legislation to expressly refer to 'AML CTF processing' *in general*, rather than specifically to processing for the purposes of compliance with 4MLD. This will also be conducive to the adoption of cohesive group-wide AML and CTF processes.

c. Data transfers to third countries

Article 39(3) and 39 (5) of 4MLD set out the circumstances in which firms may share SARs with one another, including where firms are in third countries. It is envisaged that firms can share SARs with firms in 3rd countries providing that: the other firm is in a 3rd country with equivalent AML laws, the firms are in the same professional category and are subject to data protection obligations. In the case of 3rd country branches and majority owned subsidiaries, firms are permitted to share SARs with them where these branches and subsidiaries fully comply with group policies and procedures, including data sharing.

In contrast, Article 44 of GDPR prohibits transfers of personal data to 3rd countries save for in limited prescribed circumstances including where:

- adequacy decisions have been made by the European Commission in relation to 3rd countries; or
- approved binding corporate rules, standard contractual clauses or approved industry codes with binding and enforceable commitments are used as data transfer mechanisms.

It should be noted that adequacy decisions are not currently available for every country. It can also take a significant period for binding corporate rules (which can, in any event, only be used for intra-group transfers) to be approved and transfers to courts or regulators cannot be undertaken via contracts.

In the light of the above, there would therefore appear to be a discrepancy in the way in which the regimes operate, with the effect that it may not be possible to transfer data in the circumstances envisaged in 4MLD. It would therefore be helpful if implementing legislation and guidance could clarify how these provisions are intended to operate, and indeed do so in way that is conducive to deterring money laundering and terrorist financing.

Whilst we note that Article 49(1)(d) of the GDPR sets out a derogation in relation to transfers where it can be shown that the transfer is necessary for 'important reasons of public interest', it is unclear whether this capture actions undertaken to deter money laundering and terrorist financing. Article 49(4) states that such public interests need to be 'recognised' in Union or Member State law.

Finally, by Article 48 of the GDPR, judgements or decisions by non-EEA courts, tribunals and administrative authorities are only recognized/enforceable if they are based on an international agreement. Whilst we understand the UK has opted out of certain aspects of these provisions, it would be helpful to receive guidance on how requests for information by regulators and courts for the purposes of preventing money laundering/terrorist financing should be dealt with by firms.