Federation of European Accountants
Fédération des Experts comptables Européens

European Commission
Directorate-General for the
Internal Market and Services
Rue de Spa 2
1000 Brussels

email: MARKT-AML@ec.europa.eu

19 June 2012

Ref: AML/PWE/PCO

Dear Sir or Madam,

Re: Report from the Commission to the European Parliament and the Council on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

FEE (the Federation of European Accountants) is pleased to provide you with its comments on the European Commission's report on the application of Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (third AMLD). FEE's ID number in the European Commission's Register of Interest Representatives is 4713568401-18[1].

FEE commends the European Commission's review of the third AMLD and welcomes the opportunity to participate through stakeholder consultation meetings and by providing written comments.

[1] FEE is the Fédération des Experts comptables Européens (Federation of European Accountants). It represents 45 professional institutes of accountants and auditors from 33 European countries, including all of the 27 EU Member States. In representing the European accountancy profession, FEE recognises the public interest. It has a combined membership of more than 700.000 professional accountants, working in different capacities in public practice, small and big firms, government and education, who all contribute to a more efficient, transparent and sustainable European economy.

Our comments, as set out in this letter, have been referenced with the relevant section in the EC report.

2. Application of the Directive

2.1 Applying a risk-based approach (RBA)

- **National/supranational risk assessments:** We support the timely production of risk assessments by Member States and at Supranational level, whilst cautioning that these will necessarily be high level and non-current. Such documents need to be seen as good background material to update risk assessments produced by obliged entities which are tailored to their own business, experience and environment.

- **RBA to supervision:** This is also welcomed but the RBA to supervision should not only consider the risks faced but also the level of preparedness of the entity to face those risks, i.e. a sophisticated entity may be significantly exposed to a wide range of risks, but it may be well-equipped to manage and mitigate these risks. In this context, future supervision needs to direct resources available accordingly in order to deal with those who are less well-equipped whether through resource or commitment.

- **RBA applied by Financial Institutions (FIs) and Designated Non Financial Businesses and Professions (DNFBPs)**: We consider this requirement as the key to efficient and effective application of the RBA. By putting the responsibility onto the obliged entity to select and justify the applied approach they are enabled to react appropriately, effectively and efficiently to the risks faced rather than potentially imposing a wasteful and less effective "one size fits all" approach. However this approach must provide the freedom to obliged entities to adopt risk-averse as well as risk-balanced approaches if the obliged entity considers this is more suitable to its needs and resources.

2.2 Criminalisation of ML/TF

We have no comments on this section.

2.3 Scope

2.3.1. Serious Crimes

Our comments are set out below in response to each question raised (shown in italics):

- *Whether the existing "all serious crimes" approach remains sufficient to cover tax crimes:* We consider this approach sufficient and appropriate as it incorporates all serious crimes, including serious tax crimes, as defined in the legislation of each Member State.

- *Whether tax crimes should be included as a specific category of "serious crimes" under Article 3(5):* We do not consider this necessary, as national legislation addresses the tax crimes that fulfil the criteria of a "serious crime".

- *Whether further definition of tax crimes is required:* It would be very difficult to further define tax crimes, as definitions and approaches vary among Member States. Nevertheless, if a further definition is considered to be required then, it must be very carefully described to ensure that the offence committed is that of tax evasion (that is, a deliberate or dishonest failure to disclose information as well as falsifying it) aimed specifically at depriving Member State fiscal authorities of taxation revenues that are properly due to them. Conversely, it must be clear that unintentional error in completing tax compliance steps or legitimate tax planning efforts to mitigate tax, are not criminal behaviours to be classified as "tax crime".

2.3.2 Broadening the scope beyond the existing obliged entities

We have no comments on this section.

2.4 Customer Due Diligence (CDD)

Regular CDD: Our comments are set out below in response to each question raised (shown in italics):

- *Reducing the €15,000 threshold in Article 7(b) in respect of occasional transactions; and reducing the €1,000 threshold for electronic fund transfers in Regulation 1781/2006:* We make no comment on the threshold levels but request that the new directive explicitly defines an "occasional transaction" as being in respect of an investment in a financial product, in order to ensure consistent treatment throughout the Member States.

  Seizing this opportunity, we would like to draw the European Commission's consideration on whether further clarification is necessary regarding the application of the CDD threshold in order to ensure that all professionals providing similar services are treated equally under the AML framework, irrespective of whether they are accountants or not. For example, there may be doubt as to whether the requirements of the Directive apply for the provision of tax advisory services by a lawyer, while tax advisory services provided by an accountant would be considered within the scope of the Directive.

- *Harmonising the approach to identification and/or compiling a list of EU-wide recognised identity documents issued by Member States in order to facilitate customer identification/verification:* We are not in favour of detailed provisions in the Directive specifying how identification or verification is undertaken as it would be complex and may reduce the RBA and the ability to react swiftly to developments. However, we support the provision by governments of supporting information to the regulated sector in this and other areas, such as equivalence, specified disclosure obligations, supervision for AML, PEPs, risk assessments etc.

- *Clarifying the obligations on both parties for third party reliance:* In our view the drafted clarification introduces a significant risk as it is not explicit that in a third party reliance scenario, the third party must provide comprehensive information to the person relying as to identify beneficial ownership, control etc. This may be the case not only between individuals but also between FIs and third parties. Based on our experience, it currently works effectively only within FI groups or between a few entities who have strong business relationship with

each other, as in such cases the investment in diligence of the other party (and its procedures) is worthwhile. We believe significant change is required if wide use of reliance is to occur.

Enhanced Due Diligence (EDD): With the exception of PEPs and countries on caution or sanctions lists, the requirement to carry out EDD should be part of the RBA to Due Diligence that entities are required to have and justify. National professional guidance will have a core role in this area.

Simplified Due Diligence (SDD): Our comments are set out below in response to each question raised (shown in italics):

- *Clarifying that SDD is not a full exemption from CDD*: This would be a welcome clarification.

- *Whether the Directive should set out the risk factors that need to be taken into consideration when determining if SDD is appropriate, or whether it should provide specific examples of when SDD might apply:* We believe that the new Directive should enumerate the criteria required for an entity or product to qualify for SDD. A practical example could be that entities listed on certain stock exchanges could qualify for SDD by virtue of the transparency requirements and supervision rules inherent in obtaining their listing on those stock exchanges. We consider important to set clear criteria in the Directive regarding those cases where an SDD approach may be taken, but this should be qualified by a requirement for the obliged entity to consider if there are higher risks related to a specific customer or product which renders the specific situation unsuitable for SDD. The onus should be on the obliged entity to make this risk assessment and to be prepared to justify it to its supervisor, rather than for the approach to be specified in detail in the Directive.

- *Whether further guidance on risk factors should be elaborated (for example by the AMLC in the case of the financial sector):* National professional guidance will have a key role in this regard.

- *Whether to specify (either in the Directive or via guidance) a minimum set of measures that have to be taken by the obliged entities in SDD situations:* The Directive should be clear that it is obligatory to obtain and retain documentation from an appropriate source that evidences the qualification of the entity or product for SDD.

- *Introducing, in line with the new FATF standards, a risk-based approach with respect to whether or not to apply SDD when opening a business relationship with another FI licensed in the EU or treated as an equivalent third country:* This should be applied, and additionally, based on the principles set above, consideration should be given to extend the provisions of SDD to include all government controlled bodies in equivalent countries as well as all entities subject to professional regulation and supervision for AML equivalent to EU standards in those countries.

2.5 Politically Exposed Persons (PEPs):

Our comments are set out below in response to each question raised (shown in italics):

- *Incorporating the new FATF provisions for domestic PEPs and PEPs in international organisations:* It is important to align the Directive to the FATF changes as this will assist in world-wide group compliance programmes.

- *Removing the residence criteria:* This is supported.

- *Including provisions relating to life insurance:* This is supported.

- *Clarifying that a risk-based approach should be applied to PEPs even beyond one year after they have left office:* More focus is needed on the real issue at stake, i.e. whether someone who is or has been in a politically exposed position (the period of time has less relevance, the key issue is about understanding the profile and background of the person), has obtained their wealth through legitimate sources of income available to them at the time they were politically exposed and thereafter.

- *Clarifying the definition of "senior management":* This is well defined in the UK Financial Services Authority Senior Management Systems and Controls Sourcebook glossary and the EC could take up this definition[2].

2.6 Beneficial Ownership

2.6.1. The 25% beneficial ownership threshold

We do not consider there is any evidential basis for a need to change this threshold.

2.6.2. Beneficial ownership – implementation issues

Regarding ownership interests, it should be clarified that to ascertain the Ultimate Beneficial Owner (UBO) requires the understanding of the complete upward ownership tree to the level of detail necessary to conclude if any person owns or controls 25% of the client entity by controlling the necessary percentage of its ultimate holding company. In addition, it should be explicit that in all cases there is a two stage process required, i.e. one is to ascertain the UBO, or to establish that the structure is such that there is no natural person who qualifies as a UBO while the management or executive control is a second and separate workstream which should require identification of the executive management of the entity in all cases.

2.6.3. Availability of beneficial ownership information

See our comments in paragraph 16 below.

2.6.4. Further considerations

---

[2] For the definition of "senior management" in the Financial Services Authority glossary, please refer to: http://media.fsahandbook.info/pdf/Glossary/S.pdf, page 9

Our comments are set out below in response to each question raised (shown in italics):

- *Clarifying the definition of the beneficial owner, in the light of the revisions agreed by the FATF and the AMLC's conclusions:* See our comments in paragraph 14 above.

- *Including, either into the AML Directive or in another existing legal instrument in the company law area, measures to promote the transparency of legal persons/legal arrangements:* The identification of the UBO is the most lengthy and expensive challenge in conducting work to fulfil AML obligations. Provisions to require governments to set up publicly accessible and freely accessed registries of beneficial ownership for companies and other legal arrangements would be costly, complex and impinge on numerous privacy considerations. We consider a more appropriate solution would be to commit directors of companies and other legal arrangements with the duty to at least assist in the identification of their UBO information and make it available to obliged persons and entities with whom they wish to form a business relationship (provided those person and entities are supervised for compliance with both AML obligations and professional obligations of confidentiality).

2.7. Reporting obligations

Our comments are set out below in response to each question raised (shown in italics):

- *The new EU framework could reinforce the existing provisions requiring FIUs to provide timely generic feedback to reporting entities:* We agree with this proposal but it is important to confine the required duty to generic/thematic feedback although of course individual feedback to reporters may still be provided at the FIUs discretion on an exceptional basis.

- *Introducing an explicit role for self-regulatory bodies in the reporting process (e.g. establishing guidelines):* We generally support the proposal. However, we consider there is limited value in using a regulatory body to receive and then send reports to the FIU as it increases the cost and complexity while it introduces the risks of potential delay and breach of confidentiality in the process.

- *Introducing an explicit requirement that reporting be done to the host country FIU:* We are in favour of this proposal.

- *Clarification that in cases where Member States conclude that transmission of Suspicious Transaction Reports (STRs) is being filtered, they should actively consider requiring reporting to be made direct to the FIU:* We recommend a requirement for all reporting to be provided directly from the source.

- *Reinforcing the requirement under Article 33 with respect to statistical data in order to ensure more comprehensive and comparable statistics:* We are in favour of this proposal.

2.8. FIUs

We are supportive of the suggested improvements to FIU access and co-operation but at all stages, in order to retain reporter confidence, it is vital that confidentiality of the source

of the report is assured except as ordered by a court of competent jurisdiction or by freely given consent of the reporter.

2.9. Group compliance

Our comments are set out below in response to each question raised (shown in italics):

- *The notion of "group" is currently only incorporated in Article 28(3), providing for exemptions to the prohibition of disclosure of the fact that an STR has been filed or that a ML/TF investigation is being carried out. A definition of "group" could be incorporated into Article 3 to allow a broader scope of application:* We agree that as far as information sharing is concerned the definition needs to be expanded to allow professional networks to be treated for this purpose as cross border "groups" (e.g. professional practices who belong to a network which agree to operate to common standards and adopt a common brand even though country ownership is independent and distinct). However, it would not be appropriate or feasible to enforce a requirement for group AML policies in this context as there is no common ownership and so no ability to enforce detailed national policy and procedure.

- *Introducing an explicit possibility of allowing intra-group flows of information on potentially suspicious transactions prior to the filing of a report, while respecting data protection obligations:* We are in favour of this proposal.

- *The possibility of allowing information flows to the auditors of the Head Office. Independent auditors do not fall within the definition of "group", and therefore would not benefit from the exemption in Article 28(3):* We are in favour of this proposal.

2.10. Supervision

The considerations are supported.

2.11. Self-Regulatory Bodies (in the case of the accountancy profession, national professional institutes)

We doubt whether the provision of reporting via a supervisory body has any beneficial effect on the regime. Such provision is considered unnecessary since there are clear rules for the conduct of competent authorities obliging them to maintain the confidentiality of the source of any report unless either ordered to disclose it in judicial proceedings by a Court of competent jurisdiction, or where disclosure is freely consented by the reporter.

We support the requirement on self regulatory bodies to provide guidance.

2.12. Third Country Equivalence

Our comments are set out below in response to each question raised (shown in italics):

- *Whether an equivalence regime is needed in the new Directive, in light of the increasing move towards a risk based approach:* The regime should be retained. In order to provide for proportionality regarding the burden on obliged entities, it is vital to specify clearly any broad classifications that can potentially qualify for SDD. We consider that specifying cases where SDD may be

considered applicable strongly supports a risk-based approach. We do, however, believe that clear categories for SDD should be supported through a good information flow from Member State governments. Furthermore, where obliged entities identify risk factors relating to a particular client, they need to consider whether SDD is appropriate, or whether additional steps are needed.

- *Whether the process of establishing equivalence "lists" is still needed, and if so, whether there is a role to be played at EU level (e.g. prescriptive approach to be set out in the Directive, maintaining the existing intergovernmental approach, mandating the AMLC with work in this area, etc.):* The process is vital, and the recent advances made at EU level in this regard are welcomed. We consider the approach a reasonable model and from the perspective of the regulated sector, provision of such lists is an important supporting mechanism. Whether or not it is employed at EU or Member State level, is a matter for inter-governmental discussion.

- *Whether it is still appropriate to maintain a provision in the Directive (currently Article 40(4)) on "black listing", given that this has never been used:* This approach should be retained. If the “black listing” should be used, appropriate measures would need to be taken to ensure that such list would be updated whenever necessary.

- *Whether a coordinated approach at EU level might be needed in order to coordinate measures in response to the FATF listing process:* This approach is supported.

2.13. Administrative Sanctions for Non Compliance with the Directive

We support greater harmonisation in the sanctioning regime by a set of minimum common rules to be applied to key aspects of the sanctioning regime.

2.14. Protection of Personal Data (DP)

This is an area where improvement to content and clarity is needed in the Directive. It is important going forward to be specific about retention of CDD and reporting data - CDD rules need modification as retention for 5 years after end of relationship is hard to administer and potentially disproportionate in data protection terms. It is important also to be explicit through appropriate derogations that information held for suspicion reporting is exempt from subject access requests made to obliged entities and persons as well as competent authorities provided that information is held for the purpose of reporting and in good faith. Disclosure of such information should be only by order of a court of competent jurisdiction. Although this provision is vital to protect the interests of reporters, the European Commission should also consider the protection of the interests of persons who may be subject of suspicion reports considering the principle of “presumption of innocence” as the threshold for reporting is only suspicion and not knowledge. In this respect, a time limit could be set on the retention period of such data not only by obliged entities and persons but also by the national FIUs.

3. Commission's assessment of the Directive's treatment of lawyers and other independent legal professionals

We make no comments for this section.

Thank you very much for the opportunity to comment on the report and for the extension of the deadline.

For further information on this letter, please contact Mrs Petra Weymüller, FEE Senior Manager at +32 (0)2 285 40 75 or via email at petra.weymuller@fee.be.

Yours sincerely,

Philip Johnson
FEE President