afme/
Finance for Europe

The Basel Committee on Banking Supervision
Bank for International Settlements,
CH-4002, Basel
Switzerland

Via email: baselcommittee@bis.org

27 September 2013

# Consultative Document: Sound management of risks related to money laundering and financing of terrorism

The Association for Financial Markets in Europe (AFME)[1] welcomes the opportunity to respond to the Basel Committee's Consultative Document: Sound management of risks related to money laundering and financing of terrorism.

**General Comments / Overview**

AFME Members believe that the Committee's proposals represent a significant enhancement on the standards that banks will employ in their efforts to combat money laundering and terrorist financing by providing greater clarity to banks of how they comply with the FATF Recommendations. It is apparent that the Committee has noted the lessons from reports issued by various public sector bodies in recent years and is encouraging banks to do the same. Given the broad support of AFME Members to the Committee's proposals, they, nevertheless, offer the following detailed comments on particular proposals with a view to clarifying the proposal or enhancing its effect.

**Detailed Comments**

Paragraph 21 – The three lines of defence

The Committee recommends that "the chief AML/CFT officer should, for example, not have business lines responsibilities and should not be trusted with responsibilities in the context of data protection or in the function of internal audit." Whilst AFME Members understand the basis for this recommendation, it is possible that in smaller banks, the chief AML/CFT officer may have data protection or internal audit responsibilities. AFME suggests that a combination of such duties be permitted on the express approval of the supervisor of such banks.

Paragraphs 26 & 27 - Adequate IT systems

The Committee recommends that "A bank should have IT monitoring systems in place that are adequate for the risks faced. Such IT monitoring systems should cover all the accounts and transactions for the benefit of, or by order of, the customer." Whilst AFME Members support the objective behind the recommendation, it should

[1] The Association for Financial Markets in Europe (AFME) represents a wide range of participants in European wholesale financial markets. Our members comprise all pan-European banks as well as key regional banks, brokers, law firms, investors and other financial market participants. As such we seek to bring market insight and industry perspective to the discussions on the full range of financial regulatory reform effects that are currently under way.

be left for each bank to decide whether or not it employs an IT monitoring system to review the accounts and transactions of each customer: some products and services which are offered by banks do not lend themselves to IT monitoring as opposed to manual monitoring, such as capital market transactions, correspondent banking and trade finance.

Furthermore, consistent with the adoption of the risk based approach encouraged by the Financial Action Task Force (FATF), banks should have the discretion, consistent with their individual assessment of risk, not to monitor customers' accounts in respect of certain products, services or types of customer. For example, where customers' accounts are funded by government welfare payments, the risk of money laundering may be deemed to be low. Also, saving accounts for the benefit of a child which do not mature until the child has reached the age of majority are likely to be deemed to be low risk of money laundering. The types of customers who are likely to be deemed to be low risk include those whose activities are subject to government regulation or supervision such as educational establishments maintained by the public sector or pension funds whose activities attract certain tax benefits once they have been approved by tax authorities. Accordingly, AFME suggests that banks, with the agreement of their supervisors, should be permitted not to monitor customers' accounts in certain types of products and services and not to monitor the accounts of certain types of customers.

The Committee recommends that banks' IT systems should have the ability to aggregate information by customer, product, across the group and by transactions. Given that many AFME Members have hundreds of systems in which they record customers' data and transactions across the many products and services which they offer, the building of such an aggregation function will be complex and time consuming. Accordingly, it is important that supervisors grant banks adequate time to plan, construct and test these IT aggregation systems.

Paragraphs 33 & 35 - Customer and beneficial ownership identification, verification and risk profiling.

In paragraph 33, the Committee recommends "A bank should establish a systematic procedure for identifying and verifying its customers and, where applicable, any beneficial owners." Although the Committee has made its proposals in order to support the FATF Recommendations, AFME Members believe that the Committee should clarify that the term "beneficial owner" is defined consistently with the FATF definition, i.e. a natural person who controls 25% or more of a corporate entity's voting capital or who controls the entity by other means. Without such clarification, it is possible that supervisors may interpret "beneficial owner" to include natural persons who control 1% or less of a corporate entity's voting capital.

Paragraph 33 further states that "A bank should also verify that any person acting on behalf of the customer is so authorised, and should verify the identity of that person." The customer database of AFME Members is heavily weighted towards large, multinational corporates, many of whose securities are listed on the world's major stock exchanges. To verify that the any employees of such entities have the proper authority to act on behalf of the customer would be disproportionate, particularly when most large entities conduct their transactions on an electronic basis without any physical interaction with a bank, as would be the requirement to verify the identity of such employees who have been authorised to act on behalf of the entity. With a large corporate, the number of employees authorised to act on behalf an entity numbers may be in the thousands. It is the experience of AFME Members over many years that there is no material risk arising from unauthorised

employees acting on behalf of entities such as these and other large entities. Furthermore, under EU law, where a third party deals with a person who reasonably appears to have been properly authorised to act on behalf on that entity, the third party may enforce any transaction or contract against the entity should the person not have been properly authorised to act. Accordingly, AFME Members suggest that the Committee clarify this proposal to make it clear that only in cases where one natural person acts on behalf of another natural person will there be a requirement to verify the authority provided by the second person and to verify the identity of the first person.

The final sentence of paragraph 35 recommends that "Any information collected on customer activity or behaviour be used in updating the bank's risk assessment". It is possible that supervisors and banks will interpret this recommendation to mean "all" information, regardless of whether it is significant, irrelevant, material or immaterial in terms of any one customer. Accordingly, AFME recommends that only significant or material information collected on customer activity or behavior should be used to update a bank's risk assessment, not least because, in the original recommendation, a bank would be required to collect and utilise information some of which will have no effect on a bank's risk assessment.

Paragraphs 42, 46 & 47 - Ongoing monitoring

Paragraph 42 states "Ongoing monitoring should be conducted in relation to all business relationships and transactions, but the extent of the monitoring should be based on risk identified in the bank's risk assessment." AFME Members conduct significant elements of their business with financial institutions who are regulated for money laundering purposes by financial supervisors and with central clearing houses who are also regulated by financial supervisors. Given that the fundamental premise of the adoption of the risk based approach is for banks to utilise their resources where they perceive the risks to be greatest, it may be argued that to require a bank to monitor its transactions with other regulated banks and regulated central clearing houses based in FATF or G20 jurisdictions would bring no significant benefits to the fight against financial crime. Therefore, AFME Members recommend that where a bank conducts transactions with a regulated bank or central clearing house based in a G20 or FATF jurisdiction, the requirement to monitor those transactions is dispensed with.

Whilst AFME Members understand the proposal contained in paragraph 46 to bring together, in one place, the totality of a bank's relationship, across all products and services, with each customer, the Committee should be aware that to plan, construct, implement and test such an IT system would represent a significant challenge to the banking industry. Accordingly, AFME Members suggest that the Committee provide for a significant implementation lead time for banks to implement an appropriate system. In order to minimise any delays in the introduction of such systems into individual banks, supervisors may require banks to submit regular reports to the supervisors on the progress of their respective implementations.

Paragraph 47 recommends that banks should screen their customer database using screening databases on a periodic basis to detect PEPs and other high risk accounts. AFME Members are surprised with this particular recommendation given that the FATF Guidance issued in June 2013 on Politically Exposed Persons states (at paragraph 61) "Use of these (commercial) databases is not required by the FATF Recommendations, and is not sufficient for compliance with Recommendation 12." As it appears that there is an inconsistency between the Committee's proposals and

the FATF Guidance, AFME Member suggest that the Committee revise its proposal to bring it in line with the FATF Guidance.

Paragraph 48 - Management of information

The Committee proposes in paragraph 48 that the relevant CDD information contained in documents used to verify a customer's identity be transcribed into the bank's own IT systems. Whilst AFME Members use such IT systems for these purposes, they use the IT systems in a way that complies with data protection legislation and in a manner that prevents the improper use of confidential information. Therefore, AFME Members suggest that the Committee notes that the use of such IT systems are compliant with data protection laws and procedures to prevent the improper use of confidential information.

Paragraphs 66, 69 & 70 - Consolidated AML/CFT policies and procedures

The Committee recommends in paragraph 66 "A bank should not rely on introducers that are subject to standards that are less strict than those governing the bank's own AML/CFT procedures. This will entail banks monitoring and evaluating the AML/CFT standards in place in the jurisdiction of the referring bank." This proposals requires banks to evaluate the AML/CFT standards in place in other jurisdictions and thus "second guess" the opinions of FATF and other supra-national public sector bodies who make, and publicise, evaluations of the AML/CFT standards in various jurisdictions. Private sector banks do not have the authority nor the ability to access relevant parts of the administration of a foreign jurisdiction in order to make an informed assessment of the AML/CFT standards in place. These banks should be able to rely on the public assessments of FATF and other bodies as to whether the AML/CTF standards are less strict than those prevailing in their own jurisdiction. AFME Members note that in the EU, the European Commission in other areas of financial regulation, such as credit reference agencies, prudential matters and financial benchmark indices, the Commission allows banks to rely on public sector assessments of equivalence and does not require that banks "second guess" the views of public sector supervisors. Therefore, AFME Members recommend that the Committee permits banks to rely, exclusively on the published evaluations by FATF and other bodies of AML/CTF standards in other jurisdictions.

In paragraphs 69 and 70, the Committee calls for a robust process of information sharing with the head office and appropriate operating units regarding accounts and activity that represent heightened risk. The Committee recommends that on such accounts consolidated information, not only on the customer, but also on the beneficial owners and all types of products and services across a group are aggregated. Whilst AFME Members support the Committee's objective in this respect, they, on many occasions, find that the transfer of information for AML/CTF risk management purposes is impeded by the data protection or banking secrecy legislation in place in some of the jurisdictions in which they operate. Indeed, the FATF is currently analysing the effect of data protection legislation on the fight against money laundering and terrorist financing. Accordingly, AFME Members are pleased to note that in paragraph 92 the Committee calls on all jurisdictions to ensure that any data protection or banking secrecy legislation that they have in place does not impede the fight of banks against money laundering and terrorist financing.

We would be pleased to discuss the issues covered in this submission with the Committee or to provide any further information that the Committee have raised if that would be helpful.

Yours faithfully

Denis O'Connor
Managing Director