31 July 2017

By email to FATF.Publicconsultation@fatf-gafi.org

AFME and UKF comments on the Draft Guidance for Private Sector Information Sharing

Dear Sir or Madam,

The Association for Financial Markets in Europe (AFME) and UK Finance (UKF) welcome the opportunity to comment on the Draft Guidance for Private Sector Information Sharing.

We fully agree that effective information-sharing is one of the cornerstones of a well-functioning AML/CFT framework.

We are strongly supportive of the intent of the guidance, in particular to support the effective implementation of the AML/CFT regime, through sharing of information, both in the national and international context.

We agree that general data protection requirements, particularly those without exceptions for financial crime affecting national security or the public, may impede the effective implementation of AML/CFT requirements. At the same time, we are mindful that privacy and data protection regimes exist to protect important rights which should not be displaced without good reason. We believe that there is a need for a clear alignment between AML/CFT and data protection regimes. The two sets of rules should work together rather than one being a hindrance to the other.

We have some specific comments (below) on the draft guidance on legal constraints that may inhibit the processing of information.

Our central points are as follows:

- there should be clear Recommendations and guidance to ensure that financial institutions are allowed to process information for the purposes of financial crime risk management activities
- there should be clear Recommendations and guidance on the conditions under which personal data can be transferred between financial institutions that are not part of the same group
- there should be clear Recommendations and guidance on the conditions under which personal data can be transferred to third countries, including to courts and regulatory authorities

We would be very happy to clarify any of our comments, and to meet with you to discuss them at any mutually convenient time.

Yours faithfully,

Shahmeem Purdasy
Legal and Policy Director, Financial Crime
UK Finance

Tel: +44 (0)2 072168890
Mobile: +44 (0)7 392197726
shahmeem.purdasy@ukfinance.org.uk
www.ukfinance.org.uk

Richard Middleton
Managing Director, Co-Head of Policy Division
AFME

Tel: +44 (0)20 3828 2709
Mobile: +44 (0)7584 583 122
Richard.Middleton@afme.eu
www.afme.eu

About AFME and UKF
31 July 2017

AFME
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.

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.

UKF
UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association.

Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their day-to-day activities. The interests of our members' customers are at the heart of our work.

Approach to the FATF consultation
We agree that effective information-sharing is one of the cornerstones of a well-functioning AML/CFT framework.

We consider that the draft guidance is helpful in emphasising the importance of information-sharing. At the same time we believe that changes and clarifications are needed to the FATF Recommendations and Interpretive Notes themselves to strengthen the guidance.

We set out below our specific comments on the draft guidance.

Based on these comments, we have made specific drafting proposals directly to the relevant FATF Recommendations and Interpretive Notes in redlines, which are attached.

Specific comments

Paragraph 9 of the Draft Guidance includes the statement that "Quite often, lack of a clear understanding of what is allowed to be shared and what is not also leads to caution from financial institutions about the scope of information that they can share, creating challenges for an effective information-sharing regime."

We believe that it is essential to have a clear understanding of what information is allowed to be shared. We believe this would be effectively achieved through a standalone Recommendation.

If, however, the FATF does not wish to add a new Recommendation, we believe that to appropriately mirror the quite rightly held position by FATF that information-sharing is a cornerstone of a well-functioning AML/CFT framework, there should be amendments to more than one of the Recommendations. This reflects the positon that information sharing is an important element in many of the Recommendations. This is the approach we have taken in the attached drafting proposals.

We believe that, as a minimum, Recommendation 9 should be amended and should be accompanied by an Interpretive Note. The Recommendation, Interpretative Note and guidance would work in combination to make it clear what should be shared and that there must be appropriate protections in place for those that share information.

For example, we consider that there should be a clear combination of Recommendations, Interpretive Note and guidance to ensure that financial institutions are allowed to process information for the purposes of financial crime risk management activities, and in particular for processing undertaken in order to:

1) Prevent, detect and monitor for money laundering
2) Prevent, detect and monitor for terrorism or the financing of terrorism
3) Prevent, detect, monitor and report tax evasion
4) Prevent, detect and monitor for fraud
5) Prevent, detect and monitor for bribery and corruption
6) Prevent, detect and monitor for cyber crime

The draft guidance identifies that data protection and privacy (DPP) objectives can be in tension (or indeed conflict) with AML/CFT objectives. It is important that these tensions be effectively resolved and it is made clear that it may be necessary for national legislation and guidance to restrict in a proportionate manner the rights of individual data subjects where this is in the wider public interest. Details will vary according to the jurisdiction's exact DPP laws, but broadly these exemptions may need to cover:

- Processing of 'sensitive data' (mentioned in paragraph 12(v))
- Processing of data relating to offences, including convictions and suspicions / alleged offences
- Rights to anonymity and data deletion (as mentioned in paragraph 12(vi))
- Restrictions on profiling and automated decisions
- Rights to information concerning data processing, so as to avoid 'tipping off' suspects (as per Recommendation 21)

Paragraph 11 of the Draft Guidance states that:

"The patchwork legal framework of data protection and privacy laws across jurisdictions, including lack of compliance with FATF Recommendation 18, creates implementation challenges, particularly for the

private sector in sharing information. The issue seems further compounded when there is a lack of regulatory guidance, or an inconsistent approach towards AML/CFT requirements and DPP obligations. General data protection requirements, particularly those without exceptions for financial crime affecting national security or the public, may impede the effective implementation of AML/CFT requirements. The complexity of different DPP regimes and the fear of penalties and risk avoidance may also affect availability, access, processing or sharing of information by the private sector, even when such sharing is permitted."

We agree that there are challenges for the private sector in cases where "there is a lack of regulatory guidance, or an inconsistent approach towards AML/CFT requirements and DPP obligations."

In particular, we agree with the statement that "General data protection requirements, particularly those without exceptions for financial crime affecting national security or the public, may impede the effective implementation of AML/CFT requirements."

We refer to our suggestions above in relation to paragraph 9 and we observe that Recommendations 18 and 21, with the accompanying Interpretive Notes, should be adjusted to make it clear that the STR and related information, as well as other information necessary for the prevention or detection of financial crime, is included in the group-wide programmes.

We believe that private sector information sharing with domestic policy-makers, FIU's, law enforcement, supervisors and other relevant competent authorities are key to the effectiveness of the risk based approach and guidance produced. We observe that Recommendations 1 and 2 and the accompanying Interpretive Notes should be adjusted.

Paragraph 12 iii of the Draft Guidance states that:

"**In some cases, transfer of personal data to third countries is** prohibited unless the data protection authorities of the home country confirms that information sent to the third country will be subject to satisfactory levels of data protection, using some safeguards (for instance, for transfers of data within the group, the use of Binding Corporate Rules may be approved by such authority). The absence of such a determination may affect the information exchange. While such legislation provides the derogations on grounds of public interest, often these grounds are stated to be available only for case-by-case data transfer and not for systematic transfers of information, which may require a specific legal framework. The timely flow of information in a seamless manner may be impeded by requirements to give prior notification to national data protection authorities and obtain multiple authorisations, which has an impact on information-sharing."

There is legal uncertainty in a number of jurisdictions with regard to disclosure of personal data to third countries; for example there is legal uncertainty in the EU as to whether firms established within an EU Member State may disclose information to: courts, tribunals, litigation counterparties, regulators, and other governmental bodies outside of the EEA, in the context and for the purposes of non-EEA legal disputes, regulatory investigations/enforcement proceedings and non-EEA regulatory reporting arrangements. While this example relates to EU law, the implications are of course wider.

We believe that the FATF, in its role as the international standard setter to combat ML/TF, should take this opportunity to provide guidance to the effect that, subject to appropriate due diligence by firms, transfers to third countries for the purpose of detecting and preventing criminal activity is to be permitted. The FATF guidance should then lead to guidance coming from a country's regulators and public authorities (see further below).

The FATF guidance would set out that:

- a country is required to ensure that there are appropriate exemptions or derogations to allow transfers out of their jurisdiction for these purposes;
- these exemptions or derogations can be subject to requirements to ensure proportionality and a balanced consideration of risks to the data subject, but their scope should be clear in enabling such regulatory transfers to take place.

Third country transfers of the above kind should not require the data subject's consent or depend on country-specific approval of the receiving jurisdiction (such as an 'adequacy decision' under the EU model). These transfers should also not depend on the use of special contracts. Such controls are not designed for transfers to courts, law enforcement and regulatory authorities.

Paragraph 14 of the draft guidance states that:

"In some cases, more clarity from national regulators and public authorities on how to effectively manage differing regulatory requirements would be helpful in this regard. For example, global financial institutions operating in multiple jurisdictions would benefit from clarity on the scope of the public interest derogation contained in different data protection regulations (*i.e.* the extent to which transfers of data made for the purpose of complying with anti-money laundering regulations is permissible under this derogation). National competent authorities and financial institutions should consider adopting a proactive approach in this regard to find the right balance between the legislation on both issues. A dialogue between the national authorities responsible for privacy and AML/CFT is, therefore, helpful and indeed needed, to adopt compatible and coherent policies to facilitate financial institutions taking responsibility in this area."

We fully agree that "global financial institutions operating in multiple jurisdictions would benefit from clarity on the scope of the public interest derogation contained in different data protection regulations (*i.e.* the extent to which transfers of data made for the purpose of complying with anti-money laundering regulations is permissible under this derogation)."

We agree that "a dialogue between the national authorities responsible for privacy and AML/CFT is, therefore, helpful and indeed needed, to adopt compatible and coherent policies to facilitate financial institutions taking responsibility in this area."

We believe that a way to serve this important issue is by the inclusion of text in the proposed Interpretive Note to Recommendation 9. It would be made clear that countries should ensure their regulators and public authorities provide clear guidance on how to manage differing regulatory expectations and balance the Recommendations and data privacy so that they are mutually consistent.

In relation to the section, on page 20 of the draft guidance, concerning information sharing between financial institutions that are not part of the same group, we think the examples in the FATF guidance bring to the fore three key issues. We believe that the issues should be reflected by adjustments to the Recommendations to support and underpin the non-binding guidance.

The first example relates to correspondent banking and Recommendation 13. The second example relates to inter-bank sharing agreements and Recommendation 9. The third example relates to the filing of an STR following the sharing of information and Recommendation 20.

Correspondent banking

We believe that there needs to be an alignment between information sharing in the context of correspondent banking and data protection, privacy and bank secrecy laws.

Correspondent banks often request information about their respondent banks' customers through requests for information (RFIs) where a transaction on the customer's account is flagged as potentially suspicious.

The sharing of such information by respondent banks in response to RFIs will usually be governed by data protection/privacy and/or bank secrecy/client confidentiality laws. Although there are often exemptions in data protection laws for sharing information to combat crime, it is not always clear to what extent these apply to routine requests for information in a correspondent banking context.

The FATF's Correspondent Banking guidance (CB Guidance), at paragraph 32, details the steps that correspondent banks should take to request information from respondent banks via RFIs where there are concerns regarding a particular transaction. However, the guidance does not then go on to discuss respondent banks' parallel obligations to share such information in response to RFIs. Correspondent banks also often request information that goes beyond the information that is set out in the CB Guidance.

The absence of guidance makes it difficult for respondent banks to be comfortable that they have an appropriate justification for sharing information. It is important for respondent banks to have clarity on what they are and are not permitted to share.

So the Guidance should cover the expectations on respondent banks to share information with correspondent banks when requested via a RFI.

Inter-bank data sharing arrangements

Financial institutions sometimes share data with other financial institutions under a framework agreement. Often these frameworks are coordinated by regulators and other agencies under specific legal mandates.

However, there is also scope for financial institutions to enter into framework agreements independent of any particular agency under which information is also shared between a number of different institutions.

Guidance would therefore be appreciated on the extent of information sharing expected and the logistical requirements of how that data should be shared in this less formal context where there is no direct governmental oversight.

Filing STRs

There is a risk that greater information sharing between financial institutions that are not part of the same group would lead to the multiple submissions of an STR and related information. We therefore believe that to ensure the effectiveness of the risk based approach and avoid duplication, one financial institution should be permitted to file the STR and related information on behalf of another financial institution that relates to the same customer or the same transaction, with the filing institution providing a complete copy of the STR to the other institution.

ENDS

Proposed changes to FATF Recommendations and Interpretive Notes

31 July 2017

Recommendation 1 - Assessing risks and applying a RBA

Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, including through mechanisms that facilitate regular and effective engagement with and amongst financial institutions and designated non-financial businesses and professions (DNFBPs), and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively. Based on that assessment, countries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk-based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

Countries should require financial institutions and ~~designated non-financial businesses and professions (DNFBPs)~~DNFBPs to identify, assess and take effective action to mitigate their money laundering and terrorist financing risks.

Interpretive Note to Recommendation 1

1. The risk-based approach (RBA) is an effective way to combat money laundering and terrorist financing. In determining how the RBA should be implemented in a sector, countries should consider the capacity and anti-money laundering/countering the financing of terrorism (AML/CFT) experience of the relevant sector. As part of a country's consideration of capacity and experience of a relevant sector, a country should include regular and effective engagement with that sector. Countries should understand that the discretion afforded, and responsibility imposed on,

financial institutions and designated non-financial bodies and professions (DNFBPs) by the RBA is more appropriate in sectors with greater AML/CFT capacity and experience. This should not exempt financial institutions and DNFBPs from the requirement to apply enhanced measures when they identify higher risk scenarios. By adopting a risk-based approach, competent authorities, financial institutions and DNFBPs should be able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified, and would enable them to make decisions on how to allocate their own resources in the most effective way.

2. ...

Recommendation 2 - National cooperation and coordination

Countries should have national AML/CFT policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies.

Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policy-making and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The mechanisms and, where appropriate, coordination domestically should include those with FIs and DNFBPs.

Interpretive Note to Recommendation 2

A. Obligations and decisions for countries

3. **Assessing risk** - Countries should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: (i) inform potential changes to the country's AML/CFT regime, including changes to laws, regulations and other measures; (ii) assist in the allocation and prioritisation of AML/CFT resources by competent authorities; and (iii) make information available for AML/CFT risk assessments conducted by financial institutions and DNFBPs. Countries should keep the assessments up-to-date, and should have mechanisms to engage effectively with FIs and DNFBPs, including FIs and DNFBPs engaging with one another, and to provide appropriate information on the results to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

4-6 …

7. **Supervision and monitoring of risk** - Supervisors (or SRBs for relevant DNFBPs sectors) should have mechanisms in place to facilitate regular and effective engagement and ensure that financial institutions and DNFBPs are effectively implementing the obligations set out below. When carrying out

this function, supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBPs, and take the result of this review into consideration.

8-12 ....

Recommendation 9 - Financial institution secrecy and privacy laws

Countries should ensure that financial institution secrecy laws, data protection and privacy laws, and practices do not inhibit the implementation of the FATF Recommendations. Countries should ensure that the laws and practices do not prevent the group sharing of suspicious transaction reports and related information and other information necessary for the prevention or detection of financial crime. Similarly, where the institutions are not part of the same group, countries should not prevent the sharing of such reports or information where they involve the same customer or the same transaction.

Interpretive note to Recommendation 9

Countries should ensure that the implementation of the Recommendations and data protection and privacy laws and practices are mutually consistent.

Countries should ensure national regulators and public authorities provide clear guidance to relevant sectors on how to effectively manage differing legal and regulatory expectations when identifying, assessing, understanding and mitigating money laundering and terrorist financing risks, including how to process data that strikes the balance between satisfying the RBA and is proportionate and necessary for data protection and privacy purposes. This should include the sharing of such important information across borders.

Countries should ensure that laws and practices protect FIs and DNFBPs from litigation or other risks arising from the good faith sharing of STRs and related information and other information necessary for the prevention or detection of financial crime.

Countries should encourage frameworks (whether legal, regulatory, industry or other) for the sharing of data between different financial institutions that includes clear rules and mechanisms on requests for and the sharing of data to combat money laundering and terrorist financing, as well as other financial crime.

Recommendation 13 – Correspondent banking

Financial institutions should be required, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal customer due diligence measures, to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action;

(b) assess the respondent institution's AML/CFT controls;

(c) obtain approval from senior management before establishing new correspondent relationships;

(d) clearly understand the respective responsibilities of each institution; and

(e) with respect to "payable-through accounts", be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank

Countries should ensure that respondent banks can share relevant information, including about customers and transactions, requested by correspondent banks.

Financial institutions should be prohibited from entering into, or continuing, a correspondent banking relationship with shell banks. Financial institutions should be required to satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

Interpretive note to Recommendation 13

Countries should ensure that respondent banks can share relevant information requested by correspondent banks to enable them to fulfil their obligations set out

at (a) to (e) above, without resulting in litigation or other risks when acting in good faith.

The similar relationships to which financial institutions should apply criteria (a) to (e) include, for example those established for securities transactions or funds transfers, whether for the cross-border financial institution as principal or for its customers.

The term *payable-through accounts* refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

Recommendation 18 - Internal controls and foreign branches and subsidiaries

Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for ~~AML/CFT purposes.~~those purposes. The sharing of information within the group should include filings of suspicious transaction reports and related information and other information necessary for the prevention or detection of financial crime.

Financial institutions should be required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against money laundering and terrorist financing.

Interpretive Note to Recommendation 18

1-3 …

4. Financial groups' programmes against money laundering and terrorist financing should be applicable to all branches and majority-owned subsidiaries of the financial group. These programmes should include measures under (a) to (c) above, and should be appropriate to the business of the branches and majority-owned subsidiaries. Such programmes should be implemented effectively at the level of branches and majority-owned subsidiaries. These programmes should include policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management. Group-level compliance, audit, and/or AML/CFT functions should be provided with customer, account, and transaction information, including the sharing of filings of suspicious transaction reports and related information and other information necessary for the prevention or detection of financial crime, from branches and subsidiaries when necessary for AML/CFT purposes. Adequate safeguards on the confidentiality and use of information exchanged should be in place.

5. In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, financial institutions should be required to ensure that their branches and majority-owned subsidiaries in host countries implement the requirements of the home country, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform their home supervisors. If the additional measures are not sufficient, competent authorities in the home country should consider additional supervisory actions, including placing additional controls on the financial group, including, as appropriate, requesting the financial group to close down its operations in the host country.

Recommendation 20 - Reporting of suspicious transactions

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU). This Recommendation does not prohibit countries permitting the filing of a suspicious transaction report or related information by one financial institution on behalf of another financial institution that relates to the same customer or the same transaction.

Interpretive note to Recommendation 20

1-3 ...

4. The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called "indirect reporting"), is not acceptable. The mandatory obligation could be satisfied by countries permitting one financial institution filing a suspicious transaction report on behalf of another financial institution when it concerns the same customer or transaction. Where such a filing is made, the filing institution should submit the information that it has received from the other institution. The filing institution should provide a complete copy of the report to the other institution.

Recommendation 21 - Tipping-off and confidentiality

Financial institutions, their directors, officers and employees should be:

(a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and

(b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU.

This Recommendation does not prohibit the sharing of filings of suspicious transaction reports or related information or other information necessary for the prevention or detection of financial crime as required in Recommendations 9 and 18.