baselcommittee@bis.org

**Division Bank and Insurance**
**Austrian Federal Economic Chamber**
Wiedner Hauptstraße 63 | P.O. Box 320
1045 Vienna
T +43 (0)5 90 900-ext | F +43 (0)5 90 900-272
E bsbv@wko.at
W http://wko.at/bsbv

| Your reference, Your message of | Our reference, contact person | Extension | Date |
|---|---|---|---|
| | BSBV 189/Dr.Egger | 3132 | 27 September 2013 |

# Consultation – Sound management of risks related to money laundering and financing of terrorism

The Division Bank and Insurance of the Austrian Federal Economic Chamber, as representative of the entire Austrian banking industry, appreciates the possibility to comment on the Consultative Document "Sound management of risks related to money laundering and financing of terrorism" and would like to submit the following position:

**Chief AML/CFT officer (recital 22)**
In recital 22 it is stated: "The chief AML/CFT officer may also perform the function of the chief risk officer or the chief compliance officer or equivalent."

We assume that the mentioned "chief risk officer" is accountable to the management board. Therefore the compatibility of the AML/CFT officer function with a position as management board member may only be possible in exceptional cases. Statutory provisions require that the position of AML/CFT officer should be established in such a way that the AML/CFT officer is responsible to the management board and must report directly to the board without having to go through any intermediate levels. In contrast, the wording in the guideline implies a hierarchical relationship. Additionally, given his major area of responsibility, a management board member will generally lack the necessary time to meet the full scope of obligations associated with the function of AML/CFT officer.

**Adequate IT systems (recital 26-29)**
Rec. 26 states that a bank should have IT-systems, which are appropriate in terms of the risk the particular bank faces. Though, in the following recitals (27-29) a definition is provided of what capabilities these IT-systems should have, regardless of risk and risk adequacy („changes in the transactional profile of customers", „aggregation capabilities", „management of alerts", „generation of alerts of unusual transactions" etc.).

Moreover „standard paramenters provided by the developer of the IT monitoring system" are mentioned. It seems that these parameters must not be internally developed systems.
We think it should be left in the responsibility of banks to choose the tools and methods to meet the international and national requirements to combat money laundering and terrorism financing. Neither at the EU-level nor at the FATF-level there are such claims on IT-systems. Rather the risk based approach is mentioned, which depending on the risk analysis requires appropriate measures and due diligence.

If an IT-system as the one described in the consultation paper is required for all banks, this would be overshooting, cost-intensive and would clearly go beyond the requirements set out by the FATF in its 40 recommendations.

Therefore, we argue the case for:

1. Deletion of point (d) "Adequate IT systems" (recital 26-29)
2. In case point (d) is not canceled as a whole, we would leave in accordance with the principle of proportionality the first sentence of recital 26 („A bank should have IT monitoring systems in place that are adequate for the risks faced.") and would cancel the precise definition and paragraphs.

**Customer acceptance policy (recital 31)**
Recital 31 states: "Decisions to enter into or pursue business relationships with higher-risk customers should entail enhanced due diligence measures, such as approval to enter into or continue such relationships, being taken by senior management."
An approval by senior management is explicitly required only for business relationships related to PEPs and relationships to Correspondent Banks outside the EEA. We would therefore argue not to extend this duty of approval by senior management unduly.

**Record Keeping (recital 48 and Annex 1)**
We think recital 48 is somehow overshooting. For instance, in Austria it is not required to keep copies of photo IDs. It is deemed to be adequate to save the respective ID data electronically. The requirement to retain a paper copy of the photo ID would be an additional burden for credit institutions which is unnecessary, because investigations of authorities can also start based merely on documented ID data.

Therefore, we argue the case for:

1. Deletion of (i) of recital 48
2. In this regard also in Annex 1, point II.7, 8$^{th}$ sub-point the words "and documents" should be deleted. Moreover the idea of "screening against local databases" should also be deleted, because it is excessive and too vague in terms of its meaning.

**Mixed Financial Groups (recital 79)**
In recital 79 a data transfer within a group of different financial companies (banks, insurance companies) is required. We would like to state that in this regard also national obligations of secrecy should be taken into account like local data protection and privacy laws and regulations.

Therefore we would argue to complement the second sentence in recital 79 as follows:
„Mixed groups should have the ability to monitor and share information on the identity of customers and their transaction and account activities across the entire group in accordance with their respective domestic laws, and be alert to customers and their transactions and account activities across the entire group and be alert to customers that use their services in different sectors, as described in paragraph 77 above."

Kindly give our remarks due consideration.

Yours sincerely,

Dr. Franz Rudorfer
Managing Director
Division Bank & Insurance
Austrian Federal Economic Chamber