Deutsche Bank

27 September 2013

Deutsche Bank AG
Winchester House
1 Great Winchester Street
London EC2N 2DB

Tel: +44 20 7545 8000

Direct Tel +44 20 7545 1903
Direct Fax +44 20 7547 4179

Secretariat
Basel Committee on Banking Supervison
Bank for International Settlements

CH-4002 Basel
Switzerland

baselcommittee@bis.org

DB response to Consultative Document on Sound Management of risks related to money laundering and financing of terrorism

Dear Sirs,

We appreciate the opportunity to comment on the Consultative Document on Sound management of risks related to money laundering and financing of terrorism published by the Basel Committee on Banking Supervision (BCBS).

The international debate on effective and sound Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) policies and procedures to be implemented by banks is important. The suggested guidelines and in particular the BCBS analysis of ML/FT risks in a group-wide and cross border context, provide a sound basis.

We agree that consolidated risk management with a centralized process to coordinate and apply uniform policies and procedures on a group-wide basis would be ideal to manage the bank's ML/TF risks across international operations and that group-wide AML/CFT policies and procedures should be consistently applied and supervised across a group.

However, today we are still confronted with major difficulties, streaming in particular from diverging national data protection rules, which prevent us from implementing robust information sharing policies among our head office and our branches and subsidiaries.

Therefore, in the context of current regulatory reform initiatives at EU level (especially revision of the Third AML Directive and the Regulation on Data protection), clear rules should be set out and exemptions provided from strict data protection rules for the purpose of effectively combating Money Laundering and Terrorist Financing. These exemptions should of course be subject to adequate safeguards (Chinese walls, Need to Know principle) to maintain a high level of data protection. From our understanding of the current regulatory debates and given the delicate balance that needs to be found between two diverging interests – protecting personal data and the need to process data to efficiently combat money laundering and terrorist financing - we would find it helpful if members of the BCBS could also convey appropriate messages and explanations directly to political decision makers.

Enclosed you will find our more detailed comments on specific points in the consultative document and we trust you find these helpful. Please let us know if we can provide further information.

Yours sincerely,

Andrew Procter
Global Head of Government and Regulatory Affairs

Encl: 1

Detailed comments on BCBS consultative document on *Sound management of risks related to money laundering and financing of terrorism, June 2013*

Essential elements of sound ML/TF risk management

Three lines of defence

Nr. 18: While we agree with the points mentioned on the first line of defence, we want to underline that in certain business units like those dealing with payments, a close cooperation is required with the second line of defence (AML compliance). Indeed, due to the high straight through processing rate and volume of transactions carried out, this business area heavily relies for the detection of suspicious reporting on support through IT systems but also on special intelligence available with the second line of defence.

Nr. 24: We agree that internal audit ("third line of defence") plays an important role in independently and periodically evaluating the risk management and controls within a bank. In this context we wish to underline that group audit does not write any specific policies for coverage of certain items but rather has policies for conducting risk-based audits and the coverage of AML/CTF matters would result from the risk assessment it has carried out. Of course, we would agree with the list of elements to be audited (adequacy of banks AML/CFT policies and procedures, effectiveness of bank staff, of compliance oversight and quality control and of bank's training of relevant personnel).

Adequate IT systems

Nr. 27: According to the consultative document, IT systems should have aggregation capabilities amongst other *"across group entities" (*besides *"by customer, product or transactions carried out during a certain timeframe,* etc"). We wish to stress that it is not always desirable to the full extent to carry out aggregation across the whole group in particular due to diverging national data protection rules/ banking secrecy and corporate law with which subsidiaries must comply.
For example, the German Federal Data protection law prohibits the processing of personal data except if this is allowed or requested by a rule of equivalent value (prohibitive norm with conditional authorization). We therefore stress the importance of clear rules on data processing within corporate groups in the context of the current revision of the European AML Directive and the upcoming Data Protection Regulation.

Customer acceptance policy, identification, verification, risk profiling

Nr. 30 and 35: To evaluate the client risk in the context of the customer acceptance process, it is advised that a bank should in general determine the source of income and wealth. So far however and according to FATF-40 and the Third AML Directive, this is only required in the case of politically exposed persons (PEP).

Nr. 32 ff.: With regard to Customer and Beneficial Owner (BO) identification, verification and risk profiling, the concept of *"person acting on behalf of the customer"* is regularly mentioned. We suggest the need to further define this concept in order to ensure a common understanding (e.g. would it only include authorized agents or also simple messengers or carriers?).

Nr. 41: In Germany, numbered accounts are no longer allowed (see § 154 AO (Abgabenverordnung, Fiscal Code of Germany http://www.gesetze-im-internet.de/englisch_ao/index.html) and § 24c KWG (Kreditwesengesetz, German Banking Act - http://www.gesetze-im-internet.de/bundesrecht/kredwg/gesamt.pdf)

Ongoing monitoring

Nr. 47: The periodic screening of customer databases to retroactively identify whether a customer was a PEP by using „screening databases" (PEP-lists of commercial providers) has not previously been required and would be problematic for data protection reasons. We would rather encourage national authorities to publish periodically updated PEP lists.

Management of information, record keeping

Nr. 49: The general record retention rules mentioned, correspond to the current European rules. However, it should be taken into account that e.g. in Germany an official order (e.g. from a law enforcement authority or BAFIN) is required if records are to be retained for a longer period (e.g. till the case is closed) than the legal retention period of 5 years.

AML/CFT in a group-wide and cross-border context

Risk assessment and management

Nr. 64: The reasoning with regard to cross-border risk assessment and „sub-categories of PEPs" could be misunderstood and should be further clarified. In Germany, it may be contrasted with the compromise reached by the Deutsche Kreditwirtschaft (DK, Association of German Credit Industry) with the Supervisory Authority. According to this compromise an enhanced due diligence is applicable for national PEPs, acting at national level, only in case of particular indications.
(see: http://www.die-deutsche-kreditwirtschaft.de/die-deutsche-kreditwirtschaft/kontofuehrung/geldwaescheverhinderung.html)

Consolidated AML/CFT policies and procedures

Nr. 71 and 79: It is required that groups and financial conglomerates centralise their existing monitoring functions for the identification of possible risk patterns across the group. Due to divergent data protection rules across jurisdictions, including different rules for the transmission of information to third parties, this is today extremely difficult to put into practice. (see also response above under Nr. 27)

Annex 1 – Using another bank, financial institution or third party to perform CDD

The details described on the use of another financial institution or third party to perform customer due diligence (CDD) are in part contradicting the detailed requirements existing under German Prevention of Money laundering Act (§7 GwG - http://www.gesetze-im-internet.de/bundesrecht/gwg_2008/gesamt.pdf).

Annex 2 – Correspondent banking

Nr. 6, ff: We agree that to evaluate on an ongoing basis the risks with regard to their relations to respondent banks, correspondent banks should gather sufficient information to fully understand the nature of the respondent's business and correctly assess ML/FT risks. Among the factors that correspondent banks should consider it is suggested to include *"information on any possibility of a chain of correspondent banking"*. We would recommend further clarification of this concept of "chain of correspondent banking".