German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

on the Consultative Document of the Basel Committee on Banking Supervision titled “Sound Management of risks related to money laundering and financing of terrorism”

Contact: Silvia Froembgen
Telephone: +49 30 20225- 5372
Telefax: +49 30 20225- 5345
E-Mail: silvia.froembgen@dsgv.de

Berlin, 13-09-25

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent more than 2,000 banks.

Coordinator:
German Savings Banks Association
Charlottenstrasse 47 | 10117 Berlin | Germany
Telephone: +49 30 20225-0
Telefax: +49 30 20225-250
www.die-deutsche-kreditwirtschaft.de

Comments on the Consultative Document of the Basel Committee on Banking Supervision titled “Sound Management of risks related to money laundering and financing of terrorism”

General comments on the role of the financial industry in the fight against money laundering, terrorist financing and financial crime

The consultative document of the Basel Committee on Banking Supervision titled “Sound management of risks related to money laundering and financing of terrorism”, published in June 2013, takes into account the new 40 Recommendations of the Financial Action Task Force (FATF). In a number of fields, the document, however, goes beyond the scope of the FATF-40, an aspect which in the opinion of the German banking industry harbours considerable potential for compliance risks.

Before discussing the issues in detail the German Banking Industry Committee (GBIC), the voice of the German banking industry, would like to point out that during the past decade, financial institutions have invested considerable resources in measures to combat money laundering (AML), terrorist financing (CFT) and financial crime. At present, the banking industry is by far the largest contributor to the detection of such offences. Against the backdrop of the global risks, especially after the terrorist attacks of September 2001 in the USA, the scope of the measures to prevent the laundering of drug money was extended to the prevention of terrorist financing. After the review of the 40 FATF Recommendations, they now also cover tax crime and the financing of the proliferation of weapons of mass destruction.

While financial institutions have many years of experience and are well placed to assess the money-laundering risks of certain products and to identify certain suspicious patterns of account movements, they rely to a considerable extent on external and independent sources of information (such as, for example, publicly accessible databases and company registers) in order to assess certain risk factors linked to (i) customer profiles (including correspondent banking institutions) or (ii) the ownership structure of legal entities and (iii) the beneficial owners of such entities. Past experience permits the conclusion to be drawn that the fight against money laundering, terrorist financing and financial crime can succeed only if public authorities promote greater transparency concerning information on corporate ownership structures and beneficial owners, and provide requisite support to the private sector. Another prerequisite for successful cooperation with public authorities is that the authorities publish information on politically exposed persons (PEPs), as well as on countries that fail to implement equivalent standards to combat money laundering and terrorist financing. We, therefore, believe that greater efforts by government authorities to enhance corporate transparency as well as the proportionate application of rules concerning customer due diligence that reflect the different levels of risk of customers and financial institutions’ business models could be decisive in contributing to the success of the AML/CFT regime.

Comments on the Consultative Document of the Basel Committee on Banking Supervision titled “Sound Management of risks related to money laundering and financing of terrorism”

Specific comments

In view of the general background outlined above the German banking industry wishes to make the following specific comments on key aspects of the Basel Committee’s consultative document:

Para 24: Three lines of defence

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, however, 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. Nevertheless, 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).

Paras 26–29: Adequate IT systems

Para 27 on page 6 states that bank’s IT monitoring systems should be able to aggregate information. The text in brackets specifies what these aggregation capabilities should be, namely *by customer, product, across group entities, transactions carried out during a certain timeframe, etc.* We would like to point out that, owing to local legal requirements, aggregation *across group entities* may not always be fully possible since it may conflict with national data protection rules, rules on banking secrecy or company law requirements, especially with respect to subsidiaries and participations. Therefore, we propose that this point be taken into account in para 27.

Paras 32–41: Customer and beneficial owner identification, verification and risk profiling

Paras 30 and 35 require banks to routinely identify a customer’s source of income and wealth in order to evaluate the associated risk indicators as part of its customer acceptance policy. Under the FATF 40 and the EU’s Third Anti-money Laundering Directive, by contrast, this is only necessary if the customer is a politically exposed person (PEP). Furthermore, due consideration should be taken of the fact that a substantive identification of a customer’s source of income and wealth cannot be ensured by a financial institution, especially in those cases in which

- the financial institution concerned is not the sole bank of the customer in question or
- the customer in question transfers assets from another financial institution and verification of the customer’s statements by the financial institution concerned is in most cases impossible.

We, therefore, propose to delete this requirement.

Moreover, para 35 requires the customer’s *behaviour* to be considered even when evaluating risk indicators at the outset of a business relationship. Yet it is only possible to monitor and analyse

customers’ behaviour in the course of doing business with them. At the beginning of the relationship, banks can only make a preliminary assessment on the basis of the evidence available (type of product, desired transactions, possible classification as PEP) and adjust this, if need be, in response to the customer’s actual behaviour as the business relationship develops. In our view, these aspects should be taken into account in para 35.

Paras 42–47: Ongoing monitoring

Para 47 proposes that banks periodically check their customer databases with the help of *screening databases* with a view to detecting PEPs not identified as such at the outset. Screening of this kind is not required as things stand and is likely to pose data protection problems. The question arises as to whether *screening databases* refer to PEP lists compiled by commercial providers. Should this be the case, the requirement would only entrench the current problem that in the absence of alternative sources, banks have to use commercially provided lists. It would be more appropriate if supervisory authorities or national governments published periodically updated PEP lists which could be used for the ex-post identification of PEPs.

Paras 48–52: Management of information

Para 48 sets out general record-keeping requirements. These largely reflect the legal requirements currently in force in Europe. We would nevertheless like to point out that in Germany, for instance, a court order is required at present if documents and data are to be kept for a longer period in connection with an official request for information or criminal proceedings (e.g. until the case is closed). In our view, this point should be taken into account in para 49.

Paras 64–65: Risk assessment and management

Para 64 mentions the term *sub-categories of PEP*. It is not clear what is meant since neither the FATF Recommendations nor the Third Anti-Money Laundering Directive (2005/60) use this expression as things stand. We would therefore suggest deleting the term in the interests of clarity.

Paras 66– 80: Consolidated AML/CFT policies and procedures; Group-wide information sharing; Mixed financial groups

Paras 71 and 79 require banking groups and financial conglomerates to consolidate their monitoring functions for identifying possible risks and suspicious transactions and to exchange money laundering-related information within the group. Compliance is likely to be very difficult for groups operating in several countries since data protection rules and rules on sharing information with third parties differ across jurisdictions (see also our comments on para 27).

Comments on the Consultative Document of the Basel Committee on Banking Supervision titled “Sound Management of risks related to money laundering and financing of terrorism”

Annex 2: Correspondent banking ML/FT risk assessment – information gathering

Correspondent banks are required to collect sufficient information about respondent banks which may be part of a *chain of correspondent banking* so that they can assess, on an ongoing basis, the risks associated with their correspondent banking relationships. The consultative document does not define what would constitute such a chain. Nor is it clear what is meant in the final bullet point by *any possibility of a chain of correspondent banking*. This bullet point should therefore be deleted.

* * *