European Banking Industry Committee

European Banking Federation (EBF) • European Savings Banks Group (ESBG) • European Association of Cooperative Banks (EACB) European Mortgage Federation (EMF) • European Federation of Building Societies (EFBS)
European Federation of Finance House Associations (Eurofinas)/European Federation of Leasing Company Associations (Leaseurope)
European Association of Public Banks (EAPB)

Secretariat of the Basel Committee on Banking Supervision,
Bank for International Settlement

baselcommittee@bis.org.

27th September 2013

EBIC comments on Basel Committee consultative document on sound management of risks related to money laundering and financing of terrorism

The consultative document of the Basel Committee on Banking Supervision (BCBS) 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 European banking industry harbours considerable potential for compliance risks.

The European Banking Industry Committee (EBIC) supports the work of the BCBS on the sound management of AML/CTF risks. EBIC is, however concerned by an increasingly high number of recommendations and guidelines being issued by a variety of policy-makers and supervisory bodies.

At European level, the recommendations of the FATF are integrated into the EU regulatory framework by the third Anti-Money Laundering Directive (3rd AMLD) and Implementing Measures[1]. These Directives have in turn been transposed by the various EU Member States into their national law. In line with the revised FATF recommendations dated 16 February 2012, the EU is currently reviewing its legislation in this field[2].

It is important to recognise that all organisations involved in the development of AML/CTF standards have thus far issued guidance on how general standards should be interpreted or implemented in practice. EBIC welcomes the BCBS efforts to consolidate and rationalise their previous publications on AML/CTF guidance. However, it is also crucial that the BCBS guidelines be consistent with the work already done in this field by other organisations.

Before discussing the issues in detail EBIC 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

[1] Directive 2005/60/EC *on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*, OJEU L 309/15 25.11.2005 and Directive 2006/70/EC *laying down implementing measures for Directive 2005/60/EC as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis*, OJEU L 214/29 4.08.2006.

[2] See European Commission's Proposal for a Directive *on the prevention and the use of the financial system for the purpose of money laundering and terrorist financing,* COM(2013) 45 final

EBIC Secretariat: Avenue des Arts 56 B-1000 Brussels
Tel: +32 (0)2 508 37 69 E-mail: secretariat@eubic.org
or julien.ernoult@eapb.

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. EBIC therefore believes 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.

In view of the general background outlined above, the European banking industry wishes to make the following detailed comments on key aspects of the Basel Committee's consultative document:

Para: 20 second line of defense
EBIC would like to clarify that in many financial institutions the internal control department is responsible for the fulfilment of the review of the AML process. The AML officer's duties should clearly be distinguished from the sample testing and the fulfilment of policies and procedures.

Para 22: AML Officer
The requirement in para 22 to define the relationship between a Chief Risk Officer and the AML/CFT officer could be interpreted as a possible hierarchical relationship between both function holders. It is important that the position of AML/CFT officer be established in such a way that the AML/CFT officer is responsible to senior management or the Board and must report directly to senior management or the Board without having to go through any intermediate level. It should therefore be clarified that each function is directly responsible towards senior management or the Board. EBIC stresses that the compatibility of the AML/CFT officer function with a position as management board member is only appropriate for smaller less complex institutions in light of the proportionality principle. Given his or her major area of responsibility, a management board member of a larger banking group will generally lack the necessary time to meet the full scope of obligations associated with the function of AML/CFT officer.

Para 24: Third line of defense
EBIC agrees that internal audit ("third line of defense") plays an important role in independently and periodically evaluating the risk management and controls within a bank. In this context, however, EBIC wishes 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 EBIC 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 banks' 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.* EBIC 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, EBIC proposes that this point be taken into account in para 27.

EBIC would also like to underline that relevant computer programs are useful to detect typical circumstances that indicate possible money laundering activities (cash deposits of numerous small sums or smurfing activities or other suspicious transactions) on payment accounts. Identifying unusual transactions on savings accounts which are usually not used for payment transactions, however, are not possible without further ado. On the one hand, credit institutions do not accept cash deposits of their customers on these accounts; therefore deposits only originate from accounts which were already identified in compliance with the anti-money laundering provisions. On the other hand, it is usually the customer's monthly savings which can predominantly be registered on the accounts. Extraordinary payments result usually from the contractual relationship with the customer (e.g. the repayment of a loan) which are therefore directly noticed by the staff.
Against this background, the installation of electronic monitoring systems would not be suited to detect suspicious transactions on these accounts. Therefore EBIC calls for a modification of the requirements of paras 27-29: banks should only have an obligation to set up IT monitoring systems where these bring added value to uncovering suspicious transactions.

Para 31: Customer acceptance policy

Para 31 requires enhanced due diligence for foreign PEPs. In consideration of the draft of the 4th AMLD it should be specified that "foreign" in the case of the EU means "non-EU" PEPs. Furthermore, regarding the decision to enter into or continue a business relationship with a higher risk customer, EBIC deems that senior management approval should be expressly limited to PEPs and correspondent bank relationships outside the EEA.

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 3rd AMLD, by contrast, this is only necessary if the customer is a 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.

EBIC, therefore, proposes 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 paras 30 and 35.

Para 34 Identification of customers and beneficial owners
EBIC takes note that banks may require customers to complete a written declaration of the identity and details of the beneficial owner. It is indeed important to involve the customer in the fight against money laundering and to make them liable for the accuracy and completeness of the information related to the beneficial owner. However, jurisdictions should also be involved and provide banks with the ability to access beneficial ownership information through public registers.

It does not seem appropriate to have an understanding of the occasional customer's profile and behaviour as described in para 35. There is a clear difference between an established business relationship and an occasional customer. Therefore policies should take this into account and provide for two separate procedures (e.g. different risk criteria for a regular customer and an occasional transaction).

The mechanism described in para 40 related to the estimated customer risk is only feasible if financial institutions are entitled to transfer information at the request of the financial institution accepting the customer.

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 suppliers. 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 supplied 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. EBIC would nevertheless like to point out that in many countries 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.

Para 48 also proposes that banks record the documents they receive when identifying the customer (such as passports, ID cards, driver's licenses – cf. number 36). National laws and the EU provisions have considered it as sufficient that banks transcribe the data of the ID documents electronically. The correctness of data is verified by the presentation of the identification document. This is recorded.
In practice, the electronic transcription of the customer data obtained from the identification documents is totally sufficient for the activities of the investigative authorities. It would be a burden for the institutions if they had to retain the copies of all identity documents. Further,

some credit institutions do not maintain subsidiaries but enter into contact with clients via independent sales representatives. These would have to carry along mobile copy machines in order to copy the identification document during the process of identification.
According to EBIC the provision asking credit institutions to record the copies of identity documents the banks are provided with when verifying the identity of the customer or the beneficial owner should be deleted.

Para 55 Suspicious Transaction Reports
The words "in cooperation with law-enforcement agencies or the FIU" should be deleted as the review of the relationship and the risk classification process is the responsibility of the financial institution and cannot be shared with law enforcement agencies or the FIU. It is also crucial that financial institutions receive timely and specific feedback on filed suspicious transaction reports so that financial institutions can make an informed decision.

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 3rd AMLD use this expression as things stand. EBIC would therefore suggest deleting the term in the interest of clarity.

Also, it is not always possible for financial institutions, as required by para 64, to identify customer that pose a higher AML risk across the group. This would imply a centralized database containing identification data of all the customers of all the entities of a group. Beside the technical and legal barriers (data protection) preventing the group to compile such a list, it would raise serious security concerns related to any breach of the database.

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).
It would also be more meaningful to modify these paragraphs in order to ensure adaptation of the rules to various organisations, especially those which are decentralised.

Moreover, it should be acknowledged that an institution which needs to apply customer due diligence to a customer relationship should be able to use the customer identification data of another institution with which it cooperates in market activities, provided that the institutions are both subject to the same anti-money laundering provisions.

Annex 1: Reliance on third parties

EBIC would like to underline that it is of the utmost importance to maintain the recognition of reliance on third parties and the possibility for financial institutions to fully rely on another entity which is regulated and supervised. It could be clearly established that only identity of the customer and the beneficial owner and the purpose and intended measure of relationship are required at the outset of the relationship.

Also, as evidenced by the draft guidelines, compliance with AML/CTF rules is resource-intensive. Smaller, independent or specialised firms may simply not be able to comply with these rules without the assistance of third-parties. EBIC disagrees with the BCBS that reliance on a third party in the performance of customer due diligence should be treated per se as a potential risk factor. EBIC would welcome clarification from the BCBS on this point.

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.

EBIC would also like to underline that statements in para 7 are not specific to correspondent banking but are taken into account in the global risk based approach implemented by financial institutions. It might be useful to add the words "on basis of a risk sensitive approach" after the word "consider" in the first line of the paragraph.

In the seventh bullet point in paragraph 7 the word "efforts" should be replaced by the word "framework".

In the eighth bullet point it does not seem appropriate to exchange CDD processes between financial institutions. It should be the supervisor's responsibility to assess CDD procedures and their application.

In the ninth bullet point the scope of the term "third party entities" is much too wide in this context as it could involve all clients of the respondent bank. This point should be clarified.

Para 10: in this paragraph, EBIC does not support the notion of a meeting with local regulator/ supervisor/ FIU/ relevant governmental agencies. Only the respondent bank shall have relationship with its authorities. If a bank is authorised in a jurisdiction it shall be assumed that the financial institutions comply with local regulations and specifically with AML regulation. If it is a good practice to elaborate an appropriate level of CDD of the respondent bank, there is no justification for meetings with local authorities. Another solution might be to request the supervisor to publish a list of financial institutions that are AML compliant.

The approval by a senior level of correspondent bank relationships should be subject to the risk based approach.

***