28 September 2013
Secretariat of the Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002 Basel
Switzerland

E-mail: baselcommittee@bis.org

Dear Sirs

Comments on Basel Committee on Banking Supervision *Sound management of risks related to money laundering and financing of terrorism - consultative document* (2013)

Thank you for the opportunity to comment on the above document.

The document can be an important source of guidance to supervisors and banks on management of money laundering and terrorist financing risks. In its current form the document is however too reflective of earlier documents of the Basel Committee on Banking Supervision (for example *Customer Due Diligence for Banks* (2001)) that were drafted for rule-based compliance frameworks. The impact of a proportional approach, and especially the impact of the risk-based approach that now underpins the 2012 Forty Recommendations of the Financial Action Task Force, must be fully considered and reflected in the document to ensure that it is relevant to the current challenges faced by supervisors and institutions.

It is noticeable that the document, for example, focuses on the management of higher money laundering and terrorist financing risks, but does not provide guidance on the management of lower risks, or on an appropriate risk appetite. While higher risks must be addressed by enhanced due diligence measures, the effectiveness and efficiency of the risk mitigation regime can be undermined when banks uses enhanced measures to address all risks, including lower risk. It is therefore important to guide supervisors and banks to adopt mitigation measures that are appropriate to the risks that must be managed. This version of the document makes various references to enhanced customer due diligence and even to standard due diligence processes but no reference to simplified customer due diligence.

School of Law Faculty of Business and Law
Geelong Waurn Ponds Campus, Locked Bag 20000, Geelong, VIC 3220
Tel 03 522 72215 hoslaw@deakin.edu.au www.deakin.edu.au

Consideration also needs to be given to:

- The alignment between the Basel model of customer profiling and the FATF guidance on simplified customer due diligence;
- The design of a group-wide risk management system that responds adequately and appropriately to domestic risks in host countries, including to national risk assessments of host countries;
- Ensuring that compliance with the stricter home or host country regime does not unnecessarily undermine an appropriate risk-based approach or appropriate measures to support financial inclusion initiatives and does not increase integrity-related financial exclusion risks in the home or host countries.
- Appropriate protection of privacy of customer records of host countries when accessed by home country bank employees or home country supervisors.

I enclose an attachment with more detailed questions and comments on specific statements.

Yours sincerely

Professor Louis de Koker

Questions and comments relating to Basel Committee on Banking Supervision *Sound management of risks related to money laundering and financing of terrorism - consultative document* (2013)

1 Aligning BCBS guidance and FATF guidance on financial inclusion

In 2012 the FATF adopted a risk-based approach to Customer Due Diligence (CDD) and key aspects of the AML/CFT framework. This implies that risks must be assessed and appropriate CDD measures must be adopted to mitigate the identified risks. Enhanced risk measures are required where risks are assessed as higher, while simplified CDD may be applied where risks are lower.

In the same year the BCBC adopted its new *Core Principles for Effective Banking Supervision* (2012). In terms of BCP 29 all banks should be required to "have adequate policies and processes, including strict customer due diligence (CDD) rules to promote high ethical and professional standards in the banking sector and prevent the bank from being used, intentionally or unintentionally, for criminal activities."

While BCP 29's reference to "strict" CDD applies to enhanced CDD it is less obvious that it refers to standards and simplified CDD measures too. Unless the BCBS intends to signal to supervisors to guide banks not to employ simplified CDD where appropriate, clear guidance on how and when to apply simplified CDD within the context of BCP 29 is required.

In addition to guiding supervisors on aligning the interpretation of BCP 29 with the FATF risk-based approach, guidance on aligning simplified CDD and customer profiling is also required.

The FATF's Customer Due Diligence (CDD) measures focus on the identification and verification of the customer/beneficial owner; understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and ongoing monitoring of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds. Recommendation 10 advises that financial institutions should be required to apply each of the CDD measures, but that they should determine the extent of such measures using a risk-based approach in accordance with the Recommendations.

The BCBS discussion paper (and the previous Basel guidance papers relevant to money laundering and terrorist financing) focuses on customer profiling, i.e. collecting a range of relevant information of a client to enable the bank to anticipate the normal transactional pattern of a customer. The precise fit between simplified CDD in lower risk scenarios and profiling is however not clear. Questions such as the following arise:

1.1 What is the type of information that must be collected to ensure that the profile is sufficient to support AML/CFT measures? The FATF and the BCBC appear to take different positions regarding the types of information that constitute core CDD information.

In FATF *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (2013) the following is advised:

"75. The FATF Recommendations do not specify the exact customer information (referred to by certain countries as "identifiers") that businesses subject to AML/CFT obligations should collect to carry out the identification process properly, for standard business relationships and for occasional transactions above USD/EUR 15 000. Domestic legislation varies, although common customer information tends to consist of name, date of birth, address and an identification number. Other types of information (such as the customer's occupation, income, telephone and e-mail address, etc.) are generally more business and/or anti-fraud driven and do not constitute core CDD information that must be collected as part of standard CDD—although such information could appropriately be part of enhanced CDD for higher risk situations." (par 75)

The BCBC discussion paper indicates that banks should obtain the following information to profile customers and assess the risks they pose:

"A bank should develop and implement clear customer acceptance policies and procedures to identify the types of customer that are likely to pose a higher risk of ML and FT pursuant to the bank's risk assessment. When assessing the risk, a bank should consider all relevant factors such as a customer's background, occupation (including a public or high-profile position), source of income and wealth, country of origin and residence (when different), use and purpose of accounts, linked accounts, business activities or other customer-oriented risk indicators before determining what is the level of overall risk and the appropriate measures to be applied." (par 30)

It would be helpful to address this apparent contradiction in views as to the information that constitutes "core CDD information that must be collected as part of standard CDD". In particular it would be helpful to explain clearly how that would align with simplified CDD,[1] what the minimum information is that should be gathered where product risks are assessed as low,[2] and how profiling should be done where minimal information of the customer was captured when the account was opened.

---

1 A potential solution lies in this approach identified in Bester, Chamberlain, de Koker, Hougaard, Short, Smith, and Walker *Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines* (2008) FinMark Trust/World Bank 35-36: "In one example, a country with a weak identification system accepted the national identity document as means of verifying identity but compensated for its deficiencies by requiring FSPs to collect (but not verify) further information to construct a more detailed client profile. Such information may include: nature of employment, expected levels of income, purpose of account, address, etc. In this way, the regulator has avoided imposing significant costs on the FSP that would have been incurred had they been required to build an alternative identification system. At the same time, it created a useful profile that can be used to monitor for suspicious transactions as well as for building better client relationships. The government could then initiate longer term programmes to improve the national identification system." In terms of this approach more extensive customer information is gathered but not necessarily verified. While institutions may incur costs when collecting such information, the richer customer profile is of commercial benefit to the institution as it enables it to tailor its service and offering that customer.

2 De Koker "Aligning anti-money laundering, combating of financing of terror and financial inclusion: Questions to consider when FATF standards are clarified" 2011 *Journal of Financial Crime* 18(4) 377: "Depending on the level of CDD, effective monitoring in respect of basic account-based financial

1.2 What should be the frequency of updating of customer information in relation to lower risk customers and products?

1.3 When should profiling information be collected where product risks are assessed as low? If it should be done at account opening, what measures can be taken to ensure that it does not erode the space for simplified CDD as per the FATF standards?

1.4 The BCBS discussion paper states:

"The ability of the bank to effectively monitor and identify suspicious activity would require access to updated, comprehensive and accurate customer profiles and records." (par 45).

It furthermore states:

"Only if banks ensure that records remain accurate, up-to-date and relevant by undertaking ***regular reviews*** *of existing records and updating the CDD information can other competent authorities, law enforcement agencies or financial intelligence units make effective use of that information in order to fulfil their own responsibilities in the context of AML/CFT. In addition, keeping up-to-date information will affect the bank's ability to effectively monitor the account for potential suspicious activities."* (own emphasis) (par 51)

The FATF on the other hand specifically advises that in relation to lower risk products or services may consider "(R)educing the frequency of customer identification updates". (INR 10 par 21).

It would be important to align these views.

2 Specific comments relating to the text of the discussion paper

2.1 *"In conducting a comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied."* (par 14)

Banks will only have access to publicly available information. Many smaller countries may have very limited information regarding risks factors. While countries and institutions are developing risk assessment methodologies to meet the requirements of the 2012 Forty Recommendations, it is important to be clear about the expectations of risk assessments done by banks. These assessments and especially the determination of "all relevant inherent and residual factors" cannot go beyond what is publicly available. In many countries however the available information may not be highly reliable or

---

inclusion products may challenging: If the product is anonymous or very little CDD is undertaken, the monitoring process may not be able to deliver significant benefits."

sufficiently comprehensive to support an appropriate assessment. Guidance and the assessment of risk in such cases will be helpful.

2.2 *"Therefore, to enable unbiased judgments and facilitate impartial advice to management, the chief AML/CFT officer should, for example, not have business lines responsibilities and should not be entrusted with responsibilities in the context of data protection or the function of internal audit. … (par 21) The chief AML/CFT officer may also perform the function of the chief risk officer or the chief compliance officer or equivalent. He/she should have a direct reporting line to senior management or the board."* (par 22).

While it is important that the chief AML/CFT officer is independent and do not have business lines responsibilities, the requirement raises compliance costs for a small institution. It would be helpful to reference to the Basel principles relating to outsourcing of some functions, subject to appropriate oversight by the head of compliance (BCBS *Compliance and the Compliance Function in Banks* (2005) Principle 10).

2.3 *"A bank should have IT monitoring systems in place that are adequate for the risks faced. Such IT monitoring systems should cover all accounts of the bank's customers and transactions for the benefit of, or by order of, the customer. The systems must enable the bank to check business relationships with its customers against risks and abnormal situations, which may be associated with ML or FT. … In particular, these systems should be able to provide accurate information for senior management relating to several key aspects, including changes in the transactional profile of customers. … The IT systems should also have aggregation capabilities (by customer, product, across group entities, transactions carried out during a certain timeframe, etc) and be able to handle a risk grading of customers and the management of alerts. … A bank may make use of the standard parameters provided by the developer of the IT monitoring system; however, the parameters used must reflect and take into account the bank's own risk situation. … The IT monitoring systems should enable a bank to determine its own criteria for additional monitoring, filing a suspicious transaction report or taking other steps in order to minimise the risk. The chief AML/CFT officer should have access to and benefit from the IT systems as far as they are relevant for his/her function (even if operated or used by other business lines). Parameters of the IT systems should allow for generation of alerts of unusual transactions that should then be subject to further assessment by the chief AML/CFT officer. Any risk criteria used in this context should be adequate with regard to the risk assessment of the bank. …"* (parr 26-28)

"… The systems used and the information available should support the monitoring of such customer relationships across lines of business and include all the available information on that customer relationship including transaction history, missing account opening documentation and significant changes in the customer's behaviour or business profile, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank." (par 46)

The description of the integrated management information system that a bank should have, commences with the statement that it should "be adequate for the risks faced." It then proceeds to set specific requirements for a well-developed and extensive IT system that can support mitigation of standard and higher ML/FT risks. It would be helpful to outline the minimum system requirements for an "adequate" system where the institution is small and only offers lower risk products.

2.4 *"Such policies and procedures (referring to customer acceptance) should require basic due diligence for all customers and enhanced due diligence as the level of risk associated with the customer increases."* (par 30)

A reference to simplified CDD as well is required to align the statement with the FATF's risk-based approach to CDD. The discussion of enhanced due diligence in par 30 should also be balanced with a discussion of simplified CDD.

2.5 *"Generally, a bank should not establish a banking relationship, nor carry out any transactions, until the identity of the customer has been satisfactorily verified (in accordance with any prescribed documentation requirements)."* (par 33)

This reference to prescribed documentation requirements should be broadened to reflect the FATF's verification requirements that may be met using "using reliable, independent source documents, data or information." It would align the language of par 33 with that of par 34 that reflects the FATF's broader language.

2.6 *"While the customer identification and verification process is applicable at the outset of the relationship or before an occasional banking transaction is carried out, a bank should use this information to build an understanding of the customer's profile and behaviour. The purpose of the relationship or the occasional banking transaction, the level of assets or the size of transactions of the customer, and the regularity or duration of the relationship are examples of information typically collected."* (par 35)

This information is not necessarily typically gathered in relation to low risk products that are aimed at financial inclusion. Please clarify the customer particulars that banks should gather on lower risk, standard risk and higher risk customers and align the listed information in this paragraph with the information listed in par 30.

2.7 *"A bank should obtain customer identification papers as well as any information and documentation obtained as a result of CDD conducted on the customer. This could include copies of or records of official documents (eg passports, identity cards, driving licences), account files (eg financial transaction records) and business correspondence, including the results of any analysis undertaken such as the risk assessment and inquiries to establish the background and purpose of the relationships and activities."* (par 36)

The language in this first sentence of this paragraph ("as well as") indicates that banks should obtain documentary identification. This is contrary to the FATF standards that allow the usage of reliable, independent source documents, data or information, i.e.

reference to data and information as an alternative and not merely an additional source of verification.

It would be helpful if par 36 could also provide guidance on the type of verification that can be undertaken in relation customers who access lower risk products.

2.8 *"A bank should also obtain all the information necessary to establish to its full satisfaction the identity of their customer and the identity of any person acting on behalf of the customer and of beneficial owners."* (par 37)

While phrases such as "obtain all information necessary" and "establish to its full satisfaction" apply to enhanced CDD they are not necessarily applicable to simplified CDD, where the phrases such as "reasonably required" and "reasonable satisfaction" may be more appropriate. The discussion of enhanced CDD in relation to higher risk customers in par 37 should furthermore be balanced with a reference to simplified CDD where risks are lower.

2.9 *"Additionally, where CDD checks raise suspicion or reasonable grounds to suspect that the assets or funds of the prospective customer may be the proceeds of predicate offences and crimes related to ML/FT, banks should not voluntarily agree to open accounts with such customers."* (par 38)

The suspicion itself should be reasonable too and this statement should furthermore reference any tipping-off provisions that may prevent a bank from refusing to open an account where the customer will be reported to the relevant authorities.

2.10 *"A bank can only effectively manage its risks if it has an understanding of the normal and reasonable banking activity of its customers that enables the bank to identify attempted and unusual transactions which fall outside the regular pattern of the banking activity. Without such knowledge, the bank is likely to fail in its obligations to identify and report suspicious transactions to the appropriate authorities."* (par 42)

While these statements convey the importance of appropriate CDD they raise questions in relation to new products for unbanked customers. For example, how best should a bank offering a mobile money product to advance financial inclusion form an understanding of the normal banking activity of customers who have not been banked before, using a product that has not been tested before in that country or in relation to the target community? Guidance in this regard will be helpful.

Par 42 should furthermore specifically reflect the FATF standards in relation to monitoring controls that may be applied to lower risk products and customers, especially that the degree of on-going monitoring and scrutinising transactions, may be reduced based on a reasonable monetary threshold (INR 10 par 21).

2.11 *"The chief AML/CFT officer should ensure prompt disclosures where funds or other property that is suspected to be the proceeds of crime remain in an account."* (par 43) …

"The chief AML/CFT officer should ensure prompt disclosures where funds or other property that is suspected to be the proceeds of crime remain in an account." (par 54)

In addition to proceeds of crime, both statements should also reference financing of terrorists which may be derived from legitimate sources.

2.12 *"A bank should have established enhanced due diligence policies and procedures for customers who have been identified as higher-risk by the bank. In addition to established policies and procedures relating to approvals for account opening, a bank should also have specific policies regarding the extent and nature of required CDD, frequency of ongoing account monitoring and updating of CDD information and other records. The ability of the bank to effectively monitor and identify suspicious activity would require access to updated, comprehensive and accurate customer profiles and records."*

The reference to policies regarding the frequency of account monitoring and to updating of CDD information should specifically reference the FATF's INR10 par 21.

2.13 *"Consolidated risk management means establishing and administering a centralised process to coordinate and apply uniform policies and procedures on a group-wide basis, thereby implementing a consistent and comprehensive baseline for managing the bank's risks across its international operations. Policies and procedures should be designed not merely to comply strictly with all relevant laws and regulations, but more broadly to identify, monitor and mitigate group-wide risks. Every effort should be made to ensure that the group's ability to obtain and review information in accordance with its global AML/CFT policies and procedures is not impaired as a result of modifications to local policies or procedures necessitated by local legal requirements. In this regard, a bank should have robust information sharing among the head office and all of its branches and subsidiaries. Where the minimum regulatory or legal requirements of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two."* (par 61)

Par 61 and the discussion in Chapter III of the discussion paper reflect the general BCBS approach to consolidated risk management. This approach may, however, reduce the space for financial inclusion innovation at host country level. It would be very helpful if the BCBS could consider providing some guidance that would sensitise home country supervisors and global banking groups not to read and apply "uniform" and "consistent" too narrowly in their compliance and supervisory programs. Lack of guidance in this regard may undermine a risk-based approach and exacerbate overly conservative compliance responses.[3]

A consideration of ways to limit any unintended impact on financial inclusion of the "higher standard of the two" will also be of value.

---

3 De Koker and Symington Conser*vative Compliance Behaviour: Drivers of Conservative Compliance Responses in the South African Financial Services Industry* Centre for Financial Regulation and Inclusion (2011) (http://dro.deakin.edu.au/eserv/DU:30039928/dekoker-conservative-2011-1.pdf).

2.14 Par 64 discusses group-wide risk assessment and management. Its references to higher risk customers should be balanced with references to lower risk customers too.

2.15 *"Customer acceptance, CDD and record keeping policies and procedures should be implemented through the consistent application of uniform policies and procedures throughout the organisation, with adjustments as necessary to address variations in risk according to specific business lines or geographical areas of operation. Moreover, it is recognised that different approaches to information collection and retention may be necessary across jurisdictions to conform to local regulatory requirements or relative risk factors. However, these approaches should be consistent with the group-wide standards discussed above."* (par 68)

This paragraph is very helpful but should be expanded to refer specifically to lower risk and simplified CDD in the discussion of potential adjustments.

2.16 *"Higher-risk lines of business or customer categories may require specialised expertise and additional procedures to ensure an effective review."* (par 84)

While this statement is supported in relation to higher risk customers and products, it should be noted that lower risk and simplified CDD have proved as challenging and complex. Supervisors may therefore also require specialised expertise and additional procedures to ensure an effective review of measures that were implemented – or not implemented – in relation to lower risk customers and products.

2.17 *"It is essential that all jurisdictions that host foreign banks provide an appropriate legal framework to facilitate the passage of information required for customer risk management purposes to the head office or parent bank and home country supervisors. Similarly, there should be no impediments to on-site visits to host jurisdiction subsidiaries and branches by home jurisdiction head office auditors, risk managers, compliance officers (including the chief AML/CFT officer and/or AML/CFT group officer), or home country supervisors, nor any restrictions in their ability to access all the host jurisdiction bank's records, including customers' names and balances. This access should be the same for both branches and subsidiaries. If impediments to information sharing prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisors should make it clear to the host supervisor that the bank may be subject to additional supervisory actions, such as enhanced supervisory measures on the group, including, as appropriate, requesting the parent group to close down its operations in the host jurisdiction."* (par 90)

Where a bank's head office staff are granted access to information on local customers, there should be no restrictions on them reporting such information back to head office. Such information should be subject to adequate safeguards on confidentiality and use and may be subject to applicable privacy and privilege laws in the home country. (par 91)

The Committee believes that there is no justifiable reason why local legislation should impede the transfer of customer information from a host bank branch or subsidiary to its head office or parent bank in the home jurisdiction for risk management purposes,

including ML and FT risks. If the law in the host jurisdiction restricts disclosure of such information to "third parties", it is essential that the head office or parent bank and the home jurisdiction bank supervisors are clearly excluded from definitions of a third party. Jurisdictions that have legislation that impedes, or can be interpreted as impeding, such information-sharing for ML/FT risk management purposes, are urged to remove any such restrictions and to provide specific gateways appropriate for this purpose. (par 92)

2.17.1 While access to information by home country compliance officers and supervisors is important, it is not clear what the privacy and usage safeguards are that the BCBS would tolerate, given their "no justifiable reason" statement in par 92. In *Customer Due Diligence for Banks* (2001) the BCBS stated the following in relation to access:

"However, safeguards are needed to ensure that information regarding individual accounts is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner. A statement of mutual cooperation to facilitate information sharing between the two supervisors would be helpful in this regard." (par 68)

This qualification was not repeated in the same form in this consultative document. Does this mean that customer information may now be used for purposes other than "lawful supervisory purposes" once it was accessed for any of the purposes outlined in par 87? This is an important question given that for purposes of this document the term "supervisor" might refer to financial intelligence units (FIUs) in certain countries (par 12). FIUs may be able to use such information for a range of different purposes, including data analysis and law enforcement.

The 2001 reference to protection of the information by the recipient in a satisfactory manner also appears to be watered down in the consultative document. According to par 87 "*This use of information for a legitimate supervisory need, safeguarded by the confidentiality provisions applicable to supervisors, should not be impeded by local bank secrecy or data protection laws.*" (See also par 89: "*Supervisors should ensure that information about banks' customers and transactions is subject to the same confidentiality measures as are applicable to the broad array of information shared between supervisors on banks' activities*.) This statement appears to imply that all institutions defined as supervisors in the consultative document are subject to a standard set of confidentiality provisions and that these are sufficient to provide the required level of protection for customer data too. This assumption will require stronger argument and proof that such measures are sufficiently adequate to protect the rights of customers. Guidance will also be required on the enforcement mechanisms that are available, should a breach occur.

2.17.2 What are "adequate safeguards on confidentiality and use" (par 91)? In other words, what are sufficiently "inadequate safeguards" that would amount to justification in terms of par 92 to justify barring such access?

2.17.3 According to par 87:

"In a cross-border context, home country supervisors should face no impediments in verifying a bank's compliance with group-wide AML/CFT policies and procedures during on-site inspections. This may well require a review of customer files ***and a sampling of accounts or transactions*** *in the host jurisdiction. Home country supervisors should have access to information on* ***sampled individual customer accounts and transactions*** *and on the specific domestic and international risks associated with such customers to the extent necessary to enable a proper evaluation of the application of CDD standards and an assessment of risk management practices."* (own emphasis)

According to par 90, however, there should not be "*any restrictions in their ability to access* ***all*** *the host jurisdiction bank's records, including customers' names and balances."* (own emphasis)

This apparent contradiction should be addressed. If they should only enjoy access to sampled information, guidance should be provided as to the extent of information that can be requested for purposes of a "sample".

2.17.4 The access scheme envisaged in the document provides for home country supervisors to access records in the host jurisdiction. What are the access rights of host country supervisors when information relevant to their domestic supervisory powers is held in the home country? A host country supervisor may, for example, wish to access full customer records held by the group to check whether appropriate decisions were made where an account was opened for a Politically Exposed Person in the host country when that customer has had a long-standing relationship with the head office of that institution in the home country.