September 27, 2013

Sent via email

Wayne Byers
Secretary General
Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002
Basel, Switzerland
baselcommittee@bis.org

Re: Consultative Document: *Sound management of risks related to money laundering and financing of terrorism* (bcbs 252)

Dear Mr. Byers:

World Council of Credit Unions (World Council) appreciates the opportunity to comment on the Basel Committee's *Sound management of risks related to money laundering and financing of terrorism* consultative document. World Council is the leading trade association and development organization for the international credit union movement. Worldwide, there are over 51,000 cooperatively owned not-for-profit credit unions in 100 countries with more than US$ 1.5 trillion in total assets. National and provincial credit union supervisors frequently apply the Basel Committee's international standards to credit unions even though the Committee develops these standards to apply to internationally active commercial banks.

World Council supports the Committee's proposal in most respects, including the Committee's risk-based approach to anti-money laundering and combating the financing of terrorism (AML/CFT) compliance and the guidance's endorsement of the Financial Action Task Force's (FATF) *Guidance on Anti-Money Laundering and Terrorist Financing and Financial Inclusion*[1] in Paragraph 31.

World Council, however, urges the Committee to clarify the final version of this guidance in several respects, including to make clear that financial inclusion remains important even when most members of the "general public" in a jurisdiction are not "financially or socially disadvantaged," and to clarify that it is not mandatory for institutions to use expensive vendor-created compliance software and lists when the cost of such systems outweighs the potential benefits based on the institution's complexity and AML/CFT risk assessments.

World Council's Detailed Comments

- **Risk-Based Approach:** World Council supports the Committee's risk-based approach set forth in Paragraphs 13 and 14 (risk assessments), 26 (IT systems), 42 (ongoing monitoring), 64 (risk assessment and management), and 83 (supervisory risk-based approach), as well as in Paragraph 11 of Annex 2 (reviewing and updating customer due diligence (CDD)).

- **FATF Financial Inclusion Guidance:** World Council strongly supports the Committee's express reference in Paragraph 31 to the FATF *Guidance on Anti-Money Laundering and Terrorist Financing and Financial Inclusion* and this paragraph's statement that this FATF guidance "provides useful guidelines

[1] FATF, *Guidance on Anti-Money Laundering and Terrorist Financing and Financial Inclusion* (Feb. 2013), *available at* http://www.fatf-gafi.org/topics/financialinclusion/.

on designing AML/CFT procedures that are not overly restrictive to the financial or socially disadvantaged."

- **Customer Acceptance and Access to Banking Services for the Unbanked and Financially or Socially Disadvantaged:** World Council urges the Committee to revise the statement in Paragraph 31 that "[i]t is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged" so that this sentence focuses primarily on the "unbanked" and other "people who are financially or socially disadvantaged" rather than the "general public."

  We are concerned that the "general public" language could lead some supervisors to conclude that Paragraph 31 is applicable only when a majority of the "general public" are "people who are financially or socially disadvantaged." While it may be true that a majority of the public in some jurisdictions are "financially or socially disadvantaged," especially in the developing world, financial inclusion of the "unbanked" remains a challenge in many jurisdictions where much of the "general public" is middle- and/or upper-income, including in Europe and North America.

  We urge the Committee to revise this sentence in Paragraph 31 to read:

  > "It is important that the customer acceptance policy is not so restrictive that it results in a denial of access ~~by the general public~~ to banking services~~, especially~~ for people who are unbanked and/or financially or socially disadvantaged."

- **Vendor-Created PEPs Lists:** World Council does not support the mandatory use of vendor-created lists to check for Politically Exposed Persons (PEPs), as Paragraph 47 implies, and we note that the FATF's "40 Recommendations" only require institutions to "have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person."[2] We believe that what constitutes an "appropriate risk-management system" in the PEPs context depends on an institution's complexity and AML/CFT risk profile, and does not require the use of vendor-created PEPs lists per se, especially at many credit unions.

  Vendor-created PEPs lists are expensive and often do not provide significant AML/CFT benefits at smaller institution, like most credit unions, which operate in a local community where domestic PEPs (e.g., the local mayor, local council members, local MPs, high-ranking government officials at an administrative agency served by the credit union, and so forth) are likely to be known to the institution's managers, and foreign PEPs are unlikely to become members/customers given the institution's localized business model.

  This is especially true in the case of credit unions because of credit unions' "common bond" limitations on who can become a member. Credit unions' common bond limitations on membership are typically based on a geography (e.g., persons who live or work in a particular city or province), employment by one or more specific government agencies or private companies (e.g.,

[2] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*, at 16 (Feb. 2012) ("Recommendation 12 – Politically exposed persons"), *available at* http://www.fatf-gafi.org/topics/fatfrecommendations/.

"National Health Service Employees in Scotland, North England (North East, North West and Yorkshire & Humberside) and their families living at the same address"), work in a particular trade or profession (e.g., "employees who work in the Air Transportation Industry in the United States"), or membership in an association such as a trade union. These limits on membership eligibility reduce significantly the potential universe of domestic PEPs who can join the credit union and exclude most foreign PEPs from being eligible to join or otherwise receive credit union services.

To clarify that the use of vendor-created PEPs lists should depend on an institution's complexity and risk profile, we urge the Committee to revise the second sentence of Paragraph 47 to read as follows:

> "The bank should also screen its customer database ~~using screening databases~~ periodically to detect PEP and other high-risk accounts and subject them to enhanced due diligence."

- **Adequate IT Systems:** World Council supports the statement in Paragraph 26 that "[a] bank should have IT monitoring systems in place that are adequate for the risks faced."

  We do <u>not</u> support, however, the statements in Paragraphs 27 and 28 regarding the requirements of such systems because they could place an unreasonable compliance burden on credit unions in jurisdictions where supervisors apply the Committee's standards to institutions which are not internationally active. We urge to Committee to limit expressly the application of Paragraphs 27 and 28 to internationally active banks by inserting the underlined words, below, into the first sentences of Paragraphs 27 and 28, respectively:

  > Paragraph 27: "In particular, <u>at internationally active banks</u> 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."
  >
  > Paragraph 28: "The IT monitoring systems should enable a<u>n internationally active</u> bank to determine its own criteria for additional monitoring, filing a suspicious transaction report or taking other steps in order to minimise the risk."

- **Not Opening Accounts and the Prohibition on Tipping-Off:** We are concerned the statement in Paragraph 38 that "where CDD [Customer Due Diligence] 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 [money laundering/financing of terrorism], banks should not voluntarily agree to open accounts with such customers" conflicts with the AML/CFT prohibition on institutions "tipping-off" suspects.

  Specifically, we are concerned that this sentence conflicts with FATF Recommendation 21 ("Tipping-off and confidentiality") as well as Paragraphs A(2) and A(3) of the Interpretive Notes to FATF Recommendation 10.[3]

[3] *See id.* at 19 ("Financial institutions, their directors, officers and employees should be . . . prohibited by law from disclosing ('tipping-off') the fact that a suspicious transaction report (STR) or related information is being filed with the FIU."), and at 59 ("A risk exists that customers could be unintentionally tipped off when the financial institution is

World Council believes that opening the account in this situation while simultaneously filing a Suspicious Transaction Report (STR) with the jurisdiction's financial intelligence unit would be more consistent with the FATF guidance as well as more helpful to law enforcement.

We therefore urge the Committee to delete the sentence including "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" from the final version of Paragraph 38.

- **Terrorist/Proliferation Screening and the Risk-Based Approach:** World Council supports strong and effective measures to prevent the financing of terrorism and nuclear proliferation, but we question whether mandatory checking of new and existing credit union members against sanctions and terrorism lists—as required by Paragraphs 47 and 58—is consistent with the risk-based approach to AML/CFT compliance and FATF guidance.

  FATF Recommendations 5-8, on "Terrorist Financing and Financing of Proliferation,"[4] are not independent of the FATF's risk-based approach. We note also that such checks are not cost-effective for small value accounts (taking into account the value of staff time) and that these costs can negatively affect credit unions' financial inclusion efforts.

  We urge the Committee to clarify that sanctions and terrorism list checks and ongoing monitoring may be unnecessary for small value accounts that are a low-risk for AML/CFT abuse and/or for members/customers who the institution has determined are low-risk in terms of potential ties to terrorism or nuclear proliferation efforts.

Thank you very much for the opportunity to comment on the Committee's consultative document *Sound management of risks related to money laundering and financing of terrorism*. If you have questions about our comments, please feel free to contact me at medwards@woccu.org or +1-202-508-6755.

Sincerely,

Michael S. Edwards
World Council VP and Chief Counsel

---

seeking to perform its customer due diligence (CDD) obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspected money laundering or terrorist financing operation. Therefore, if financial institutions form a suspicion that transactions relate to money laundering or terrorist financing, they should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR.").

[4] *See id.* at 13 ("C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION").