World Council

August 20, 2013

Summary and Request for Comment on Basel Sound Management of Risks Related to Money Laundering and Financing of Terrorism

Executive Summary

The Basel Committee on Banking Supervision has released for public comment a consultative document entitled *Sound management of risks related to money laundering and financing of terrorism*. The Basel Committee will be accepting comments on the consultative document until September 27, 2013.

The consultative document proposes revised guidelines for combatting money laundering and financing of terrorism, including:

1. Essential requirements for a comprehensive anti-money laundering/countering the financing of terrorism (AML/CFT) compliance program;
2. Risk assessments and AML/CFT policies;
3. Customer Due Diligence (CDD) requirements;
4. CDD performed by third parties; and
5. Ongoing monitoring and reporting of suspicious activities and transactions.

The Basel Committee's *Sound management of risks related to money laundering and financing of terrorism* is intended to provide bank supervisors with guidance on AML/CFT compliance to compliment the AMT/CFT guidance of the Financial Action Task Force (FATF), such as the FATF's "40 Recommendations" for combatting money laundering and financing of terrorism (ML/TF). Credit unions are typically subject to the same AML/CFT requirements as banks.

Please provide any comments that you may have on this proposal to VP and Chief Counsel Michael Edwards (medwards@woccu.org; fax: +1-202-638-3410) by September 20th.

1. Essentials for comprehensive ML/FT Risk Management

Comprehensive risk AML/CFT management policies require the identification and analysis of the ML/TF risks present at credit unions. Comprehensive AML/CFT management also requires effective implementation of the policies and procedures that the credit union adopts to control the identified risks. The following elements are proposed as the "essential" components of a credit union's AML/CFT compliance program:

- **Assessment of All Material AML/CFT Risks:** Credit unions should consider all relevant inherent and residual risk factors at the country, sectorial, and business relationship levels in order to determine its risk profile and the appropriate level of enhanced AML/CFT measures to be applied.

- **Policies and Procedures for Customer Due Diligence**: The institution's risk-assessment (e.g., through a risk-assessment matrix) and resulting risk profile should address risk in all of these areas: (a) customer acceptance, (b) customer identification, (c) monitoring of the business relationship and (d) operations (i.e. products and service offered).

- **Member-Focused Risk Assessment:** Credit unions should also develop a thorough understanding of the inherent money laundering and financing of terrorism risks present in its membership, based on the products and services offered.

- **Jurisdictional Risk Assessment:** The credit union should also consider the AML/CFT risks associated with the jurisdiction(s) within which the credit union and/or its members do business. For example, if the credit union operates in a jurisdiction with high levels of drug trafficking and/or terrorism, its AML/CFT risk assessment should account for those risks and identify steps to lessen them. This risk assessment should include a basic understanding of the credit union's specific operational and transaction data associated with operations in a particular jurisdiction, along with other internal information collected by the credit union as well as external sources of information (e.g., national risk assessments and country reports from international organizations).

- **Corporate Governance:** Effective ML/FT risk management requires proper governance arrangements, in particular the requirement for the board of directors to approve and oversee the policies for risk, risk management and compliance is fully relevant in the context of ML/FT risk.

- **3 Lines of AML/CFT Defense:** An institution should have three "lines in defense" as part of its AML/CFT compliance program:

    1. **AML/CFT Policies and Procedures:** Policies and procedures on how to keep the activity of credit unions in compliance with AML/CFT regulations should be clearly specified in writing and communicated to employees.

    2. **Ongoing Monitoring by Compliance Officer:** The Chief Officer of AML/CFT, and/or an outside party should have the responsibility for the ongoing monitoring of the fulfillment of AML/CFT duties by the credit union.

    3. **Internal Audit:** The internal audits process consists of evaluating the credit union's risk management under the responsibility of an audit committee of the board, supervisory committee, or a similar oversight body through periodic evaluations of the effectiveness of compliance with AML/CFT policies. Credit unions should establish policies for conducting audits of the adequacy of AML/CFT policies and procedures in addressing the following: identified risks, the effectiveness in implementing policies and procedures, the effectiveness of compliance oversight and quality controls, and the effectiveness of the institution's employee training.

2. Risk Assessment and Understanding AML/CFT Policies

- **Risk Assessment Including All Relevant Factors:** In assessing risks, a credit union should identify all relevant risk factors including geographical location, patterns of transaction activity, and usage of products and services. The institution should use this information to establish criteria for identifying higher-risk members.

- **Identification of PEPs and Other High Risk Members:** The risk assessment should identify members, who pose a high risk to the credit union, including any members who are politically exposed persons (PEPs). The information collected in the assessment process should be used to determine the level and nature of the overall membership's risk and support the design of appropriate controls at the credit union and any affiliates to mitigate these risks.

    - **Member-Focused Risk Assessment:** Credit unions should have a thorough understanding of all risks associated with its members across the institution and any affiliates, either individually or as a category, and should document and update these on a regular basis commensurate with the level and nature of the risk.

    - **PEPs:** "[W]hile PEPs constitute a higher-risk customer category that is applicable across a group, the specific risks associated with sub-categories of PEPs may vary by jurisdiction."

- **Reliance on Third-Party CDD and other AML/CFT Procedures:** There should be legal clarity to the extent to which AML/CFT legislation allows credit unions to rely on CDD and other AML/CFT procedures undertaken by other intuitions that refer business to the credit union, such as in the context of an indirect lending relationship. A credit union should not rely on CDD performed by introducers which are subject to AML/CFR standards that are less strict than those governing the credit union's own AML/CFT procedures. (See section 5 of this summary for more discussion of third-party CDD.)

- **Information Sharing at the Credit Union and Its Affiliates:** Information sharing should be sought out on a centralized basis within the credit union and its affiliates (including any subsidiaries). Subsidiaries should be required proactively to provide the head office with information concerning higher-risk customers and activities relevant to AML/CFT standards, and respond to requests for account information from the head office. The group's overall ML/FT risk management function should evaluate the potential risks posed by activity reported by the credit union's branches and subsidiaries, etc., where appropriate to assess the group-wide risks presented by a given customer.

- **AML/CFT Compliance's Relationship to Prudential Supervision:** The supervisors of credit unions are expected to comply with *FATF recommendation 26:* "For financial institutions subject to the core principles, the regulatory and supervisory measures that apply for prudential purposes, and which are relevant to money laundering and financing of terrorism, should apply

in a similar manner for AML/CFT purposes." Supervisors should also apply the Basel Committee's *Core Principles for Effective Banking Supervision* to institutions' ML/FT risk management in a manner consistent with and supportive of the supervisor's rules.

- **Risk-Based Approach for AML/CFT Compliance:** There should also be the adoption of a more risk-based approach to supervising credit unions' ML/FT risk management.
    - **Supervisors Must Understand the Theory of the Risk-Based Approach:** This approach requires supervisors to develop a thorough understanding of the risks present in the jurisdiction and their potential impact on supervised entities.
    - **Supervisors Must Understand the Credit Union's Business:** Supervisors must also assess the risks present in the target credit union to understand the nature and extent of its business, and should use this operational knowledge of the credit union to evaluate the adequacy and effectiveness of its AML/CFT risk mitigation.
    - **Assign Examiners Based on Expertise:** Credit union examiners with greater AML/CFT expertise and experience should be assigned to examine credit unions with higher ML/FT risks.

3. Customer Due Diligence Process

- **Risk-Focused CDD:** The credit union's CDD policies should help control the risks identified in the credit union's AML/CFT risk assessment.
- **Consider Risks of Each Potential Member:** Credit unions should consider the nature and level of risk presented by a potential member when determining the extent of the applicable due diligence measures.
- **Verification of Identity:** Credit unions should verity the identities of members, including identities of the beneficial owners of any legal entity members and the identities of persons acting on behalf of members, using reliable, independent source documents, data or information. When relying on documents (e.g., passports, identity cards, driving licenses), credit unions should be aware that the best documents for verification of identity are those most difficult to obtain illicitly or to counterfeit. Other methods of member identity confirmation, such as checking reference with other financial institutions and obtaining financial statements, should be used when appropriate based on the credit union's AML/CFT policies and risk assessment of the member.
- **Do Not Open Accounts for Suspicious Potential Members:** The credit union should not voluntarily agree to open an account for a potential member if CDD checks raise reasonable grounds to suspect that the assets or funds of the prospective member may be the proceeds of predicate offences and crimes related to ML/FT.

- **Checking for PEPs, Terrorists:** Credit unions should also have in place procedures and material capacity enabling its front office to identify PEPs (by checking vendor-created lists of PEPs) and any terrorist- or nuclear proliferation-designated entities (by checking national blacklists such as the U.S. Treasury's Specially Designated Nationals List).

- **Incomplete CDD:** When a credit union is unable to complete CDD measures, it should generally not open the account, commence business relations, or perform any transactions. However, under certain circumstances it can be permissible for CDD to be completed after the establishment of the business relationship (e.g., because it would be essential not to interrupt the normal conduct of business). Delayed CDD completion can be acceptable so long as the credit union adopts adequate risk-management procedures with respect to the conditions and restrictions on the member's use of credit union services until CDD is complete.

- **Members Must Use Their Real Names:** A credit union should not conduct ongoing business with a member who insists on anonymity or who gives a fictitious name. Nor should confidential numbered accounts function as anonymous accounts, but they should be subject to exactly the same customer due diligence procedures as all other customers' accounts.

- **Terrorist Screening is Not Risk-Based:** Terrorist screening is not a risk-sensitive due diligence measure and should be carried out irrespective of the risk profile attributed to the customer. For this purpose, credit unions may adopt automatic screening systems. A credit union should freeze without delay and without prior notice the funds or assets of designated persons and entities.

- **IT Systems:** Credit unions should be able to ensure they have the appropriate IT systems—commensurate with its asset size, organizational structure, operational complexity, and risk assessment—to provide the credit union's business units and compliance officers with timely information needed to monitor members' accounts. These systems should be able to support the monitoring of customer relationships across all lines of business with regards to member relations, transaction history, missing account opening documentation, and significant changes in the member's financial behavior or business profile.

4. Third Parties and Customer Due Diligence

In some countries, credit unions are permitted to use third parties, such as financial institutions or other entities, to perform CDD as part of AML/CFR compliance. These arrangements can take various forms but in essence usually fall into one of the following two situations:

1. **Referral of Third Party's Existing Customer:** In these situations, the third party will usually have an existing business relationship with the customer, and the credit unions may be exempt from applying their own CDD measures at the beginning of the relationship depending on the facts and circumstances (including whether or not the third party's information seems reliable). The FATF standards permit reliance on third-party CDD for the following purposes:

- Identifying the customer and verifying that customers' identity using reliable, independent source documents, data or information.
- Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is.
- Understanding the obtaining of information on the purpose and intended nature of the business relationship.

2. **Outsourcing of CDD Compliance Procedures:** Credit unions may also use third parties to perform various elements of their CDD obligations on a contractual basis, i.e. as an outsourcing arrangement. For the reliance on third parties in an outsourcing arrangement, there should be clear policies and procedures on whether and when it is acceptable and prudent to rely on an outside party. Relevant criteria for assessing the reliance of an outside party should include:
    - The third party or parties should be as comprehensively regulated and supervised for AML/CFR purposes as the credit union, have comparable customer identification requirements at account opening, and have an existing relationship with the potential member.
    - There should be an arrangement or understanding in writing acknowledging the credit union's reliance on the third party's CDD process.
    - The credit union should consider any adverse public information about the third party, such as if the third party is subject to an enforcement action for AML deficiencies or violations.
    - Credit unions should identify and mitigate any additional risk posed by reliance on multiple parties rather than a direct relationship with one entity.

5. Ongoing Monitoring and Reporting Suspicious Transactions

- **Ongoing Monitoring is "Essential:"** The Basel Committee views ongoing monitoring as an essential aspect of sound ML/FT risk management.
- **First Identify "Normal" Member Behavior:** A credit union must have an understanding of the normal and reasonable activity of its members to enable it to identify attempted and unusual transactions which fall outside the regular pattern of banking activity.
- **Looking at More than One Line of Business to Spot Risk Patterns:** Credit unions should not only monitor members and their transactions, but should also carry out cross-sectional product/service monitoring (i.e. analyzing more than one line of business at once, such as looking at both credit card and current/checking account activities) in order to identify and mitigate emerging risk patterns.

- **Establishing Suspicious Activity Scenarios:** In establishing scenarios for identifying suspicious transactions, credit unions should consider the customer's risk profile developed as a result of the bank's risk assessment, information collected during its customer due diligence efforts, along with other information obtained. Using CDD information, credit unions should be able to identify transactions that not appear to make any economic sense, or that involve large amounts of cash deposits that are not consistent with normal or expected transactions of the customer.

- **Clear Procedures for Identifying, Reporting and Investigating Suspicious Activities:** Reporting of suspicious transactions through ongoing monitoring and reviewing of accounts will enable credit unions to identify suspicious activity, and report faulty transactions. The process of identifying, investigating and reporting suspicious transactions should be clearly illustrated with a clear description of obligations and instructions for analysis.

- **Terrorist Financing Profile:** The financing of terrorism has its own specificities that credit unions should take into due consideration. Funds that are used to finance terrorist activities may be derived either from criminal activity or from legal sources, and the nature of the funding sources vary according to the type of terrorist organization involved, with transactions usually being conducting in very small amounts.

- **Directives to Freeze Assets:** Credit unions should be able to identify and enforce funds that are subject freezing decisions—such as because the owner of the funds is wanted by law enforcement and/or is on the jurisdiction's terrorist blacklist, etc.—made by the competent authority. The credit union should not do business with any terrorist or other designated entities or individuals, consistent with their national legislation.

Questions:

1. Do you think that the proposed "essential" elements of AML/CFT compliance discussed in section 1 of this summary are appropriate and/or should additional elements be added?

2. Do you support the proposed "risk-based approach" to AML/CFT compliance?

3. Do you support the proposed "3 lines of defense" for AML/CFT of (1) policies and procedures; (2) ongoing monitoring; and (3) internal audit?

4. Do you support the proposition that screening for terrorists should not be risk-based even though most other areas of AML/CFT compliance would be risk-based?

5. What are your views on the requirement to check potential members against vendor-created lists of PEPs (which credit unions normally must pay to use)?

6. Do you have comments about the proposed CDD measures' potential impact on financial inclusion of the unbanked, such as in the case of incomplete CDD because a potential member lacks the necessary government-issued identity card, etc.?

7. Do you have concerns about the requirement not to open accounts voluntarily for "suspicious" potential members?

8. What do you think about the proposed framework for reliance on a third party's CDD and/or for outsourcing of CDD compliance functions?

9. What are your views concerning the proposed requirements for ongoing monitoring of members' financial activities using the credit union, including cross-sectional product/service monitoring (i.e. analyzing more than one line of business at once)?

10. Do you have concerns about cost and/or regulatory burdens regarding any other aspects of this proposal? If so which ones?