Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002
Basel, Switzerland
Attention: Secretariat

Re: Comment Letter on Consultative Paper, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism*

Dear Sirs:

The Clearing House Association L.L.C.[1] is pleased to comment on the Basel Committee on Banking Supervision's consultative document, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism* ("Consultative Document"), which has been issued by the Committee to support the adoption by member countries of the *International Standards on Combating Money Laundering and the Financing of Terrorist* ("FATF Standards"), which were adopted in their current form by the Financial Action Task Force ("FATF") in 2012. The document also rationalizes the Committee's previous guidance on money laundering and terrorist financing by updating and superseding prior guidance.

The Clearing House and its member banks strongly support international standards on money laundering and terrorist financing. We believe that global standards are important because money laundering and terrorist financing are global problems that must be addressed on a global basis. Many of our member banks are global institutions that face particular difficulties in dealing with different standards that apply in different countries leading to potential liability from conflicting duties and responsibilities. Moreover, different standards in different countries or regions can result in opportunities for criminals and terrorists to find weak links that they can take advantage of. We also strongly support the Committee's emphasis on a uniform, global,

[1] Established in 1853, The Clearing House is the nation's oldest banking association and payments company. It is owned by the world's largest commercial banks, which collectively employ 1.4 million people in the United States and hold more than half of all U.S. deposits. The Clearing House Association is a nonpartisan advocacy organization representing—through regulatory comment letters, amicus briefs, and white papers—the interests of its owner banks on a variety of systemically important banking issues. Its affiliate, The Clearing House Payments Company L.L.C., provides payment, clearing, and settlement services to its member banks and other financial institutions, clearing almost $2 trillion daily and representing nearly half of the automated-clearing-house, funds-transfer, and check-image payments made in the United States. See The Clearing House's web page at www.theclearinghouse.org for additional information.

risk-based approach, which we firmly believe is the only one that will work—a zero-tolerance approach will diffuse bank compliance making it less effective and ultimately impairing national and global AML and CFT efforts.

While we support the overall approach, we do have some comments on the specifics of the proposal, particularly in the areas of customer due diligence ("CDD"). In general, The Clearing House believes that any CDD rule should explicitly recognize that a rigid, unvarying approach will not work in all situations and sound rules and policies should expressly permit institutions to categorize accounts and customers based on their assessment of risks posed by the particular customer and product involved. One line of demarcation could be between mass market retail accounts (e.g., consumer checking accounts, consumer loans, and credit cards) and managed account in which a relationship manager is assigned to oversee the bank's relationship with the customer.

Any CDD rule should recognize that institutions will differ based on their customer bases, lines of business, and the kinds of products and services they offer. Institutions should, therefore, be given considerable latitude in determining the appropriate level of CDD and designing monitoring systems to discover suspicious activity. Rules should also encourage financial institutions to gather information that is needed to identify those customers that present the highest risk for money laundering, terrorist activity, or other criminal activity, so that monitoring resources can be focused on them rather than on lower risk customers.

SUMMARY

1. The Clearing House agrees that banks should include the assessment and management of money laundering and terrorist financing risks as part of their overall risk-management. Both banks and their supervisors should also acknowledge that:

   (a) Banks are in the best position to judge the risks presented by their businesses and customers, and supervisors should not substitute their judgment for that of the bank.

   (b) Bank boards should approve overall AML and CFT risk policies and should oversee management's compliance with these policies, but a board cannot be expected to manage the bank's day-to-day AML or CFT compliance.

   (c) While banks should have a set of systems that cover all accounts, customers, and transactions, there are significant practical and legal

impediments to establishing a single, unified IT system that can provide a comprehensive view of all a customer's accounts and transactions.

2. The Clearing House supports risk-based customer acceptance policies and procedures to identify high-risk customers. Such policies and procedures should apply a three-tiered approach consisting of basic identification, basic due diligence to allow the bank to categorize the customer's risk, and enhanced due diligence for high-risk customers.

3. The Clearing House believes that there should be no overall requirement to obtain or verify beneficial ownership information for all customers.

4. While we support on-going monitoring of customers and transactions, this requirement should be confined to the bank's own customers, and we strongly suggest that the Committee clarify in the final paper that banks are not expected to obtain information on the "normal and reasonable banking activity" for each of their customers from the customers themselves.

5. We agree that banks should report suspicious activity and freeze assets as required by applicable law. We also agree that banks should screen customers against applicable lists of known terrorists and other blocked persons, but we caution that such screening should not raise unreasonable expectations regarding the ability of CDD procedures to identify money launderers or terrorists.

6. We urge the Committee to encourage its member countries to harmonize their laws to allow banks to share all information in their possession throughout their organizations without regard to national borders.

DETAILED COMMENTS

1. Essential Elements of Sound AML-FT Risk Management.

(a) Assessment, Understanding, Management, and Mitigation of Risk

The Clearing House agrees that banks should include the assessment and management of money laundering and terrorist financing risks as part of their overall risk-management. Both banks and their supervisors should also acknowledge that:

- **Banks are in the best position to judge the risks presented by their businesses and customers, and supervisors should not substitute their judgment for that of the bank.**
- **Bank boards should approve overall AML and CFT risk policies and should oversee management's compliance with these policies, but a board cannot be expected to manage the bank's day-to-day AML or CFT compliance.**
- **While banks should have a set of systems that cover all accounts, customers, and transactions, there are significant practical and legal impediments to establishing a single, unified IT system that can provide a comprehensive view of all a customer's accounts and transactions.**

ASSESSMENT AND UNDERSTANDING OF RISKS. The Clearing House and its member banks agree with the Committee that in a risk-based system, the first task is to identify the risks that are presented by the various factors of a bank's business (product risks, kinds of customers, countries).[2] It should be clear, however, that a bank and its employees are the parties that are in the best position to understand and evaluate the risks that its businesses face and customers present and that judgments regarding these risks and the procedures needed to identify them will have to take account of the specific situation of each bank. Therefore bank regulators and examiners should not substitute their judgments for those of bank management and employee unless it is clear that the bank completely failed to meet any reasonable standards for assessing its risks.

PROPER GOVERNANCE ARRANGEMENTS—BOARD OF DIRECTORS' RESPONSIBILITY. We agree that the board has overall responsibility to set strategic direction and oversee management and therefore should have an understanding of the overall risk faced by the organization; we also agree that the board should get periodic reports on the bank's compliance with all statutes and regulations as well as the organization's compliance with its own policies. But it must be clearly recognized that the board is not and cannot be responsible for day-to-day management. The board's responsibility is to set broad strategic direction, appoint professional managers who are responsible for carrying out and implementing that direction, approve the policies developed by management to adhere to the goals set by the board, and in general oversee management's performance.[3] Board oversight

[2] Consultative Document at 4.

[3] *See*, Clearing House Assoc., *Guiding Principles for Enhancing Banking Organization Corporate Governance* (Jun. 2012), available at http://www.theclearinghouse.org/index.html?f=073631; *see also*, Group of Thirty, *Toward Effective Governance of Financial Institutions* (Apr. 2012), available at http://www.group30.org/images/PDF/Corporate%20Governance%20050913.pdf; Basel Committee on

of the organization's AML and CFT compliance efforts and performance falls squarely within this scheme, and boards should therefore not be expected to become involved in the day-to-day management of a bank's AML or CFT activities.

We also recommend that the Committee take guidance from the Federal Reserve Board's policy on compliance-management programs[4], which Provides that "[t]he board has the responsibility for promoting a culture that encourages ethical conduct and compliance with applicable rules and standards, and

> The board should be knowledgeable about the general content of the compliance program and exercise appropriate oversight of the program. Accordingly, the board should review and approve key elements of the organization's compliance risk management program and oversight framework, including firmwide compliance policies, compliance risk management standards, and roles and responsibilities of committees and functions with compliance oversight responsibilities. The board should oversee management's implementation of the compliance program and the appropriate and timely resolution of compliance issues by senior management. The board should exercise reasonable due diligence to ensure that the compliance program remains effective by at least annually reviewing a report on the effectiveness of the program. The board may delegate these tasks to an appropriate board-level committee.[5]

We believe that this strikes the correct balance in the responsibilities between board and management.

THREE LINES OF DEFENSE. The Committee describes three lines of defense that it believes financial institutions should have in order to cope with the threats of money laundering and terrorist financing: (i) clearly specified written policies and procedures that are communicated to all employees; (ii) a chief officer in charge of who is responsible for ensuring the bank's compliance with all AML and CFT laws and regulations and the bank's own policies and procedures; (iii) independent audit to ensure effective compliance.[6]

Banking Supervision, *Principles for Enhancing Corporate Governance* (Oct. 2010), available at http://www.bis.org/publ/bcbs176.pdf.

[4] Board of Governors of the Federal Reserve System, SR 08-8 (Oct. 16, 2008), available at http://www.federalreserve.gov/boarddocs/srletters/2008/SR0808.htm.

[5] *Id*. at 7-8.

[6] Consultative Document at 5-6.

In general, The Clearing House believes that what is defined in this section as "lines of defense" are better described as "pillars of an AML program," consistent with how this has historically been required by FATF Recommendation 18 and various AML program laws and regulations. In terms of levels of defense, The Clearing House believes that the Federal Reserve policy on compliance that we referred to in the prior section should inform the Committee's approach in this area as well. The Federal Reserve provides that:

1. Large banking organizations should implement a firmwide approach to compliance risk management and oversight.
2. Large, complex banking organizations should have compliance staff that is appropriately independent of the business lines.
    (a) Where compliance staff is located within business lines, they should have independent reporting lines to senior management.
    (b) Compensation and incentive programs should be structured to avoid undermining of the compliance staff.
    (c) Banking organizations should have corporate oversight of compliance staff within business lines to identify and address potential conflicts of interest.
3. There should be robust compliance monitoring and testing to identify weaknesses in the compliance program.
4. "The board, senior management, and the corporate compliance function are responsible for working together to establish and implement a comprehensive and effective compliance risk management program and oversight framework that is reasonably designed to prevent and detect compliance breaches and issues."[7]

ADEQUATE IT SYSTEMS. The proposal sets out a requirement at bank IT systems be designed so that they cover all accounts of all bank customers and all transactions.[8]

Banks do have systems covering all accounts, customers, and transactions, but there is rarely a single system that will at a glance give a comprehensive view of all a customer's transactions and relationships across all product lines. Most financial institutions have different systems for different products (banking, securities, etc.). Moreover, banks may, as a practical or legal matter, be required to have different systems for different countries to comply with individual countries' data-protection

[7] SR 08-8

[8] Consultative Document at 6.

laws, which often require banks to maintain information on local customers within the jurisdiction. The Committee and national regulators should therefore not underestimate the immense practical and legal impediments to establishing unified IT systems that can provide a comprehensive view of all of a customer's accounts and transactions.

We believe that for many banks having multiple systems that will each give a partial view of a customer's transactions will allow the bank to identify and take appropriate actions with respect to possible money laundering and terrorist financing, so long as the various systems taken together are reasonably designed to provide the bank with the data it needs to identify possible criminal activity and take appropriate action. Banks should therefore have discretion to choose the IT systems that will be best designed to address their individual business lines, customer base, and organizational structure.

We also note that different countries also have different definitions of accounts than the expansive definition of account (i.e., virtually any kind of relationship between a bank and a customer) that is prevalent in the United States,[9] and we believe that a standard approach to the types of customer relationships and transactions that are covered by global money laundering and terrorist financing standards should be adopted to avoid confusion on the part of banks and their regulators and to ensure that consistent policies are followed by all institutions worldwide.

(b) Customer-Acceptance Policy

The Clearing House supports risk-based customer acceptance policies and procedures to identify high-risk customers. Such policies and procedures should apply a three-tiered approach consisting of basic identification, basic due diligence to allow the bank to categorize the customer's risk, and enhanced due diligence for high-risk customers.

The Committee states that there should be clear customer acceptance policies and procedures to identify high-risk customers and that these policies and procedures should require basic due diligence for all customers and enhanced due diligence for high-risk customers.[10] The Clearing House supports clarifying CDD standards in order to provide a uniform framework for compliance, examination, regulation, and enforcement across the financial-services industry.

---

[9] *See, e.g.,* 31 U.S.C. § 5318A(e)(1)(A).

[10] Consultative Document at 7.

The Clearing House believes that there should be a three-tiered overall approach to the acceptance of customers and CDD that provides for:

1. Basic identification of the customer, which would apply to all customers and would consist of collecting from the customer enough information to allow a bank to form a reasonable belief as to the identity of the customer.

2. Basic due diligence, which would apply to all customers and consist of collecting sufficient information to enable the institution to conduct a risk analysis of the customer to categorize the level of risk the customer presents to the institution. Based on the risk rating the institution assigns to the customer, the institution would determine what additional information on the customer would be needed by line-of-business and customer category and the level of on-going transaction or account monitoring that would be appropriate and whether the customer should be moved to the next step of due diligence.

3. Enhanced due diligence ("EDD") would be required for certain customers considered to be high risk for money laundering and terrorist financing. Within this category, EDD standards should be established in accordance with a risk-based analysis for different lines of business and customer types. For example, credit-only customers will have a very different profile from customers that use demand deposit accounts to make payments; similarly, investment banking clients will have very different profiles from money services businesses using products and services, such as deposit accounts. Consideration must also be given to the method of customer on-boarding, whether the customer is dealing with a relationship manager or is a mass-market customer, and whether a customer is being on-boarded through a trusted intermediary.

The Clearing House strongly supports a risk-based approach for customer acceptance policies and procedures. A risk-based approach permits financial institutions to continue to focus on those customers and combinations of customers and products that pose the highest money-laundering or terrorist-financing risk to a particular bank and has strong support of FATF. Thus, a bank's policy should be permitted, for low-risk customer relationships, to have policies that allow for the acceptance for all customers unless certain conditions are met (e.g., identity cannot be verified, the customer is a match—or is associated with—a designated terrorist or other sanctioned person.

(c) Customer and Beneficial Owner Identification, Verification, and Risk Profiling

The Clearing House believes that there should be no overall requirement to obtain beneficial ownership information on all customers.

IN GENERAL. The Committee reiterates the FATF view that banks should be required to "identify the customers and verify their identity, unless the country has determined through a risk assessment that particular types of activities (and customers associated with the activities) may, on a limited basis, be exempted because there is a proven low risk of ML or FT."[11]

Individual customers or customer with joint accounts held for family or household purposes are almost always held in the names of the individuals who apply for the account. The Clearing House believes that banks should be required to identify those customers so that they have a reasonable basis for knowing who the customer is. Nevertheless, unless the bank comes into the possession of facts that clearly indicate that the purported customer is not in fact the beneficial owner, it should be able to satisfy the requirement to identify beneficial ownership by identifying the persons named on the account documents.

With respect to entity accounts, The Clearing House supports a reasonable requirement to obtain information on the beneficial owners, but we do not believe that a universal requirement is necessary, useful, or practical. This position is supported by FATF Recommendation 1, which states in part that

> [c]ountries should apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified. This approach should be an essential foundation to efficient allocation of resources across the anti-money laundering and countering the financing of terrorism (AML/CFT) regime and the implementation of risk based measures throughout the FATF Recommendations. Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.[12]

---

[11] *Id.*

[12] FATF Standards at 11.

Moreover, FATF Recommendation 10, which sets out recommended CDD measures, also has a beneficial ownership component, but as in Recommendation 1, the recommendation is subject to a risk-based approach.[13]

The Clearing House believes that the Committee should not adopt a blanket requirement to obtain beneficial ownership information for all accounts; it should be applied under a risk-based approach. In any event, any beneficial owner identification rule should have broad exceptions.

For example, low-risk entities that are exempt from a country's customer identification program should also be exempt from beneficial ownership identification requirements, and other specific low-risk customers (e.g., publicly traded companies, regulated financial institutions, government agencies, designated systemically important financial market infrastructures, certain licensed or regulated professionals) should also be excluded from the beneficial owner identification requirement as these kinds of customers generally pose low risks of money laundering or terrorist financing.

Any requirement to obtain beneficial ownership information should apply to new customers, with retroactive application only to existing customers that are judged to be high risk. For example, a financial institution could be required to get beneficial ownership information on an existing customer if monitoring or some other trigger event indicates a problem.

DEFINITION OF BENEFICIAL OWNER. The Consultative Document does not define the term *beneficial owner*, which is a crucial point and needs to be done carefully so that banks are clear who the regulators regard as the beneficial owner. In the case of accounts opened or maintained by intermediaries, there is a wide variety of ownership arrangements that can be difficult to encompass in regulations (e.g., trusts, nominees, escrow agents, etc.).

In particular, correspondent banks should not be regarded as intermediaries in the sense that the account balance is held to be the asset of the customer's customers or that the customer's customers are held to be the beneficial owners of the account balance. Banks open correspondent accounts with other financial institutions for their own business purposes, which will often include making payments for their customers and making payments for their own account, with all of these transactions being paid out of the one account. The balance in a correspondent account is always a debt that the bank owes to its correspondent customer; the correspondent customer's customers never have any claim against the bank for any balance in the account, even if the

[13] *Id*. at 15.

account is used to execute payments or provide other services for those customer's customers. There may be a legitimate concern that the correspondent customer is providing services for money launderers or terrorists, but that concern is best handled through transaction monitoring rather than creating the fiction that the balance in the account is owned by someone other than the correspondent customer.

VERIFICATION. The Consultative Document states that "the identity of customers, beneficial owners, as well as persons acting on behalf of customers should be verified using reliable, independent source documents, data or information,"[14] and suggests or sources that would be acceptable (based in part on the difficulty of counterfeiting obtaining illicit copies). But the Consultative Document is not clear on what it is that is being verified.

Verification can have two possible meanings: (i) verifying the identity of the individual identified by the customer as the beneficial owner of the account, i.e., verifying the *existence* of the identified beneficial owner; or (ii) verifying that the individual identified by the customer as the beneficial owner, is indeed the beneficial owner of the customer, i.e., to verify the *status* of the identified individual.

There are significant problems with verifying the status of an individual as owner of an entity. If a customer's representative informs a bank that X is a beneficial owner of the customer, there is no reasonable or practical way for the bank to conclusively prove that X actually is a beneficial owner during the customer on-boarding process, and even after-the-fact verification presents substantial difficulties. First, in most cases, the person opening the account on behalf of the customer is likely to be the only reliable source of information on beneficial ownership. There are no registries of corporate ownership in the United States, and while some—by no means all—other countries do have corporate registries, they are rarely if ever complete, often list corporate officers or registered agents rather than beneficial owners, and are almost never updated after the initial filing. Without reliable, readily available databases of corporate ownership, there is no reasonable or practical way for a bank to obtain sufficient information—independent of the information that the customer provides—to form a reasonable belief that a given person is a beneficial owner of a corporate customer. Because of this we believe that banks should not be required to verify the status of a person as a beneficial owner of a legal-entity customer. We also question the utility of verifying the identity of the person identified as a beneficial owner in most cases because identification of that person's identity would still not establish that the purported owner is actually the beneficial owner.

[14] Consultative Document at 8.

Our suggestion is that in opening an account for a non-exempt legal entity, a bank should obtain from the person opening the account the names of the entity's beneficial owners but that the institution be permitted to rely on the representative's statement about the customer's beneficial owners and not be required to verify either the identity or status of those owners, unless the institution's risk-based procedures provide otherwise. The bank will then apply its usual customer on-boarding procedures, as required. If these procedures turn up information that calls into question the beneficial ownership information obtained during the account opening process, this will prompt further investigation by the institution and may result in the filing of a suspicious activity report and may ultimately result in the closing of the account.

(d) On-Going Monitoring

While we support on-going monitoring of customers and transactions, this requirement should be confined to the bank's own customers, and we strongly suggest that the Committee clarify in the final paper that banks are not expected to obtain information on the "normal and reasonable banking activity" for each of their customers from the customers themselves.

The Consultative Document states that

> [o]ngoing monitoring is an essential aspect of effective sound ML/FT risk management. A bank can only effectively manage its risk 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 banking activity.[15]

While we agree that on-going monitoring of customers and transactions is an essential component of an AML program, we believe that the requirement should be confined to the bank's own customers and transactions that the bank actually processes. A bank should not be expected to monitor its customers' customers or aggregate the transactions that a remote party sends through multiple institutions even if all or most of those institutions direct their transactions through the bank (e.g., funds transfers that those institutions send through the bank as correspondent). In most cases, if those customers are acting as intermediaries, they will be regulated entities that should have their own customer monitoring obligations and compliance procedures.

[15] *Id*. at 10.

The Consultative Document also states that "[u]sing CDD information, a bank should be able to identify transactions that do not appear to make economic sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer."[16]

While banks do seek to understand the nature of their relationship with their customers and to determine the risk that a customer presents to the institution, this may not in all cases require asking a customer about what the customer believes is the nature and purpose of the account. In many cases, institutions are able to anticipate the level of activity in the account because this will be inherent in the nature of the product or service being offered and the type of customer using the account. In many cases, especially with respect to retail customers, the bank will have a better idea than the customer of the kinds and volumes of transactions that can be anticipated to pass through the account. In these circumstances, asking the customer to estimate the account activity will not yield much useful information and will only result in administrative burdens for the bank and the customer. Banks have significant experience with developing systems to identify unusual activity and can leverage that experience to determine the appropriate thresholds at which to determine particular transactions deviate from "normal and reasonable" for its population of customers. We therefore strongly suggest that the Committee clarify in the final paper that banks are not expected to obtain information on the "normal and reasonable banking activity" for each of their customers from the customers themselves, but can make reasonable estimates of their own based on the kind of account, the kind of customer, and the bank's own experience in providing these services.

(e) Management of Information

UPDATING INFORMATION. While we agree that banks should update their customer information files as needed, they should have the discretion to determine when updating is necessary based on their assessment of their customers' risks. These updates should be undertaken on a sliding scale depending on the risk assessment made of the customer. For example, high-risk customers could be reviewed annually or any other time that new information comes to the bank's attention (perhaps because of a change in account activity), but the account files for moderate risk customers would be updated less frequently, perhaps once every few years; low-risk customers, such as the typical mass-market retail accounts, would not be updated unless there is some triggering event, such as when the customer seeks to obtain a new service from the bank.

[16] *Id*.

(f) Reporting of Suspicious Transactions and Asset Freezing

We agree that banks should report suspicious activity and freeze assets as required by applicable law. We also agree that banks should screen customers against applicable lists of known terrorists and other blocked persons, but we caution that such screening should not raise unreasonable expectations regarding the ability of CDD procedures to identify money launderers or terrorists.

The Consultative Document touches on requirements to report suspicious transactions and freeze assets when necessary.[17] We note that banks are required to report suspicious activity under the laws of many jurisdictions. How that reporting is to be done and under what circumstances should be a matter of applicable law. Likewise, the laws of various countries require banks to freeze assets or block transactions and freeze the proceeds of the blocked transactions. Banks should follow applicable law in these cases as well.

The Committee notes that

> [f]inancing of terrorism has similarities compared to money laundering, but it also has specificities that banks 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 may vary according to the type of terrorist organisation. In addition, it should be noted that transactions associated with the financing of terrorists may be conducted in very small amounts.[18]

The Committee goes on to state that

> CDD should help a bank to detect and identify potential FT transactions, providing important elements for a better knowledge of its customers and the transactions they conduct. . . . Before establishing a business relationship or carrying out an occasional transaction with new customers, a bank should screen customers against lists of known or suspected terrorists issued by competent (national and international) authorities. Likewise, ongoing monitoring should verify that existing customers are not entered into these same lists.[19]

---

[17] *Id*. at 12.

[18] *Id.*

[19] *Id*.

We agree that banks should screen potential customers against applicable lists of terrorists and other blocked person, and that when the relevant government adds persons or entities to its lists banks should check their existing customer bases against the amended lists for appropriate action if any existing customers are listed. The checking against lists of known terrorists is the best way that CDD helps identify FT transactions, by positively identifying a customer as a match against the list. Nonetheless, the fact that banks do this screening should not raise unreasonable expectations regarding the ability of CDD procedures to identify money launderers or terrorists. Such persons arrange their affairs to escape detection, often using false names, front or shell companies, and the like to make themselves appear to be legitimate bank customers. Many terrorists will conduct their financial affairs in such a way that they are indistinguishable from any other normal customer. While there are examples of financial institutions cooperating proactively with law enforcement agencies to prevent terrorist attacks, it would not be realistic to expect financial institutions to be able to identify every single case. It is generally not until after a terrorist attack occurs that potential indicators can be assessed. In these cases, banks will maintain records that will allow an investigation into the financial conduct of the terrorists. Even well-designed CDD programs and procedures (including screening) will often fail to identify these people. The fact that these customers can evade bank controls and obtain access to bank services is not in itself an indication that a bank's CDD program is inadequate.

2. AML-CFT in a Group-Wide and Cross-Border Context

We urge the Committee to encourage its member countries to harmonize their laws to allow banks to share all information in their possession throughout their organizations without regard to national borders.

We agree that global institutions must manage their money laundering and terrorist financing risks on a global, enterprise-wide basis. An effective enterprise-wide AML-CFT program requires information to be freely shared across the organization in both directions, i.e., from local offices to the head office (to alert the head office to suspicious activity and law enforcement inquiries regarding specific customers or transactions) and from the head office to the local offices (to allow issues discovered in one locality to be disseminated throughout the organization).

Local laws, however, commonly restrict the free flow of data among various parts of a banking organization, both for financial privacy reasons and to keep sensitive law enforcement information within the jurisdiction of law enforcement authorities.

While these laws reflect the policy preferences of the countries that place a higher value on these concerns than on the concerns of banks that must protect the institution from money launderers, terrorists, or other criminals, these laws will have to be harmonized for the Committee's goal of true global, enterprise-wide compliance programs is to be achieved.

The Committee's suggestion that financial groups consider closing offices in countries that do not permit proper implementation of these information-sharing standards is not practical for all countries. Restrictive laws are too wide spread and are even found that in countries that are not on FATF's list of high-risk and non-cooperative jurisdictions.

We urge the Committee to encourage its member countries to harmonize their laws to allow banks to share all information in their possession throughout their organizations without regard to national borders.

3. Role of Supervisors

The Clearing House strongly agrees with the Committee that "[s]upervisors should adopt a risk-based approach to supervising banks' ML/FT risk management."[20]

A risk-based approach, properly understood, requires that supervisors understand their role as supervisors and realize that they are not managers and will never know as much of a bank's business, customers, or markets as the bank's management knows, and that therefore they must not substitute their judgment of appropriate risk management for the bank's management's considered judgment. A risk-based approach is not intended to catch 100% of all illicit activity—such a system is impossible. Supervisors should therefore not treat an isolated miss as a reason to call into question the effectiveness of a bank's entire AML-CFT risk management systems.

* * * * *

[20] *Id.* at 17.

We hope these comments are helpful. We would be pleased to help arrange meetings between the Committee and experts of our member banks so that we can assist the Committee. If you have any questions about any of the matters discussed in this letter, please contact me at joe.alexander@theclearinghouse.org or 212-612-9234.

Very truly yours,

Joseph R. Alexander
Senior Vice President, Deputy General Counsel, and Secretary

cc: The Honorable David Cohen
U.S. Department of the Treasury

Jennifer Shasky Calvery, Esq.
Financial Crimes Enforcement Network