

Association Comments on Risk-Based Approach for Anti-Money Laundering Standards, September 2002

By Email and Overnight Delivery

August 30, 2002

FATF Secretariat
2, rue André Pascal
75775 Paris Cedex 16
FRANCE

Re: Review of the FATF Forty Recommendations Consultation Paper

Ladies and Gentlemen:

The Securities Industry Association (“SIA”), the Futures Industry Association (“FIA”), and the Investment Company Institute (“ICI”) (the “Associations”)¹ jointly represent many of the largest non-bank financial institutions in the United States that are addressed in the Forty Recommendations promulgated by the Financial Action Task Force. Together, the Associations represent members of the securities industry, the futures and commodities trading industry, and the mutual funds industry. The Associations appreciate the invitation by FATF to comment on the Review of the FATF Forty Recommendations Consultation Paper issued on May 30, 2002 (“Consultation Paper”). We submit this joint comment letter to express the areas of interest and concern to our industries (hereafter, collectively, the “securities and related industries”).

The Associations and their member institutions are committed to assisting the government of the United States and international cooperating bodies such as FATF in deterring and preventing money laundering and terrorist financing. We are eager to assist FATF in developing international anti-money laundering (“AML”) standards that promote uniformity and efficacy while respecting the unique concerns of each jurisdiction and particular financial industry. To this end, the Associations have worked with the United States Treasury Department (the “U.S. Treasury”) and the other U.S. financial regulatory agencies to help develop appropriate regulations to combat money laundering. In addition, the Associations or their self-regulatory organizations, in consultation with the Associations, have developed AML compliance papers and/or best practices in their respective areas.

The Consultation Paper recognizes that the Forty Recommendations and the Guidance on Customer Due Diligence for Banks of the Basel Committee on Banking Supervision (“Basel Committee CDD Paper”), to which it frequently refers, were formulated within the context of the banking industry. FATF therefore requests commentary on potential revisions to the Forty Recommendations as applied to non-bank financial institutions. Because we represent the major U.S. financial institutions in the securities and related industries, we can provide that perspective with respect to the following issues: 1) Verification of identification and how it applies to (a) situations involving non-face-to-face contact, (b) use of databases maintained by reliable vendors as a method of verification, (c) the timing for obtaining verification, (d) verification of existing accounts, (e) simplified verification for low risk scenarios and (f) special verification procedures for trusts and other corporate vehicles; 2) Intermediaries and the ability of financial institutions to rely on them for purposes of meeting their verification obligations; 3) Correspondent banking/payable-through accounts; 4) Politically Exposed Persons; and 5) Suspicious transaction reporting.

I. Verification

II. Intermediaries

III. Correspondent Banking/Payable-Through Accounts

IV. Politically Exposed Persons

V. Suspicious Transaction Reporting

Initially, we believe it important to note that all of these issues should be analyzed under the rubric of a risk-based approach. We appreciate the fact that FATF has recognized the utility of such an approach when establishing an AML regime. The Associations strongly believe that a financial institution can implement an effective AML program only by conducting an assessment of the varying risks associated with the different types of businesses, clients, accounts and transactions it handles. This approach makes it more likely that resources can be focused on those customers, accounts and transactions that are most vulnerable to money laundering and terrorist financing. If financial institutions are required to devote uniform effort to all account and transaction monitoring, it will result in inefficient resource allocation and may well increase the risk that unlawful activity goes undetected.

We note that the U.S. Treasury has also adopted such a risk-based approach in various rules proposed under the USA PATRIOT Act.² These AML provisions include proposed and interim final rules on enhanced due diligence for private banking and correspondent accounts,³ interim final rules on AML programs,⁴ the final rule on suspicious transaction reporting for broker-dealers⁵ and the proposed rules for identification and verification of customers.⁶ We also note that the Financial Services Authority in the United Kingdom has adopted such a risk-based approach.⁷

We also appreciate FATF's recognition that the guidance it cites most often for best practices with respect to due diligence, the Basel Committee CDD Paper, is drawn from practices in the banking industry. We believe that many concepts adopted in the Basel Committee CDD Paper, such as verification before account opening and collection and review by the "primary institution" of an intermediary's verification documentation, are unworkable and unnecessary and, in many instances, extremely burdensome, for our member institutions.

Given current industry practice and adequate alternative safeguards in the securities and related industries, such requirements are not necessary. For example, in the context of full-service firms, a securities, futures or mutual fund account can be opened and regularly serviced by a specific individual broker who has contact with the customer and thus establishes a direct line of on-going communication—a factor not normally present in the banking industry. In other contexts, firms use other types of processes, such as sophisticated computer-based processes, to verify their customers. These processes allow the firm the opportunity to discover facts that are inconsistent with the identification information provided by the customer.

We address other distinctions between the banking industry and the securities and related industries throughout this letter. To further aid in this task, we are enclosing with the hard copy of this letter the AML best practices guidances issued by the SIA AML Committee and the National Association of Securities Dealers,⁸ the AML Interpretive Notice issued by the National Futures Association,⁹ and an AML compliance paper by the ICI.¹⁰ Additionally, the Associations would be willing to assist FATF in developing any further AML guidance that relates to our respective industries.

I. Verification

A. Non-Face-to-Face Contact

In the Consultation Paper under section 3.3, entitled "Higher risk customers or transactions," FATF addresses non-face-to-face financial services. FATF notes that there is a potentially higher risk of money laundering where there is little or no face-to-face contact with the customer. However, non-face-to-face account openings are well-accepted throughout the financial services industry, because they afford customers—the vast majority of whom are entirely legitimate and law-abiding—a convenient and cost-effective way to establish financial relationships.

Indeed, lack of face-to-face contact has long been common in the securities and related industries. For example, brokerage and futures accounts traditionally have been opened over the telephone, and mutual fund accounts almost always are opened directly by phone or by mail or by referral from a securities firm.¹¹ Although brokers sometimes meet with their customers, whether institutional or individual, they gather significant amounts of information relating to the customers to satisfy stringent regulatory obligations and conduct non-documentary verification, often utilizing databases containing identification, credit and other financial information and/or interactive query verification techniques that in many ways are superior to face-to-face documentary methods.

Broker-dealers obtain most or all of the following information upon the opening of an account: customer's name and residence; whether customer is of legal age; signature of the registered representative (broker) introducing the account and signature of the member or partner, officer, or manager who accepts the account; if the customer is a corporation, partnership, or other legal entity, the names of any persons authorized to transact business on behalf of the entity; the customer's employment data, investment objectives, affiliation with and/or accounts at other broker-dealers or financial institutions; information regarding how the account was acquired; and income and asset information. In addition, for certain other accounts, broker-dealers must make reasonable efforts to obtain, prior to the settlement of the initial transaction in the account, the customer's tax identification or Social Security number, the occupation of the customer and name and address of the employer.

Similarly, members of the futures industry are required under U.S. regulations to obtain information about their customers, which—depending on the type of customer—includes most or all of the following: the customer's name, address, age, principal occupation or business, name of guarantor, name of person controlling the account, and estimated annual income and net worth.

For FATF to recommend heightened due diligence for all or most non-face-to-face scenarios without a recognition of this historic method of doing business is likely to have grave consequences for the securities and related industries and their ability to continue their businesses, as well as for customers who will lose the benefits of being able to open accounts in a convenient and cost-effective manner. It also would disrupt the Associations' current risk-based AML approach, which would negatively affect the ability of the Associations' member firms to combat money laundering and terrorist financing by diverting resources to accounts that are not necessarily more vulnerable to money laundering risks.

FATF suggests several alternate revisions of its standards, to address the perceived risk with respect to non-face-to-face contact. The options range from requiring member countries to adopt measures to address dealing with customers electronically and over the telephone, to requiring that countries adopt several measures from an approved list, with the opportunity to provide supplemental measures as needed.¹²

The Associations believe that any measures to address the risks that arise in non-face-to-face contexts should be premised on a risk-based approach and left entirely to the discretion of the member country, which will be familiar with the practices of its financial services industries. This is because the “Know Your Customer” rules and other safeguards employed by the financial services sector vary significantly by industry, company, type of account and business. Unless FATF wishes to assemble an extensive list of verification measures that vary by industry, any more limited, mandatory list that emphasizes traditional verification measures in the banking industry risks undermining longstanding practices from highly regulated and reputable segments of the non-banking industries.

B. Verification Using Databases Maintained by Reliable Vendors

Section 3.2 of the Consultation Paper, entitled “The Customer Due Diligence Process,” contains a proposed amendment to the FATF standards that will make more explicit the required due diligence process for financial institutions. One of the provisions requires financial institutions to “[v]erify the customer's identity using reliable, independent source documents, data or information.”

As described above, the Associations' member firms often utilize reliable outside vendors that provide databases containing verification information for individuals, such as date of birth, address, Social Security number, credit history, media coverage and whether the individual falls under the U.S. Treasury's Office of Foreign Asset Control's designations of “specially designated nationals” or “blocked persons.” Equivalent verification information is provided with respect to corporations. Because such databases contain comprehensive and independent data that are widely recognized as reliable, verification based on these databases is highly informative and in some instances more thorough than a review of source documents or the face-to-face confirmation procedures used in other contexts. The Associations recommend that the amendment with respect to due diligence make explicit the ability to utilize reliable identification databases as a means of verification.

C. Timing of Verification

FATF addresses the point in the customer relationship at which verification must take place. Section 3.6.2, entitled “Timing of verification of identity,” provides three options. Option One would require financial institutions to verify their customer's identity either before a relationship is established (as set forth in the Basel Committee CDD Paper), or before the customer is able to withdraw any funds from or conduct transactions in the account. Option Two would allow financial institutions to open accounts without having verified the customer's identity so long as they do so “as soon as reasonably practicable.” Option Three would require FATF to issue best practices guidelines, with both an expectation that verification would usually take place before the opening of the account, and an understanding that there would be exceptions. The guidelines would include a list of factors for determining whether the customer should be able to withdraw funds prior to completion of the verification process.

In the securities and related industries, there are varying categories of customers, ranging from individuals—to small, private companies—to large, publicly-traded companies and financial institutions. Each category requires a different type of verification, warranting different timetables. For example, financial institutions that are well-known, publicly-held institutions may be subject to swift verification by reference to a public website. In contrast, verification of the beneficial owners of a privately-held company previously unknown to the financial institution may take longer and require personal contact with the customer. Depending on the level of risk assessed, a financial institution may choose not to open an account prior to verification. Alternatively, if the financial institution chooses to open the account during the verification process, it may still elect to place limits on the account, such as restricting the number or value of transactions.

The Associations recommend that financial institutions be permitted flexibility with respect to both the means and timing of the verification, consistent with a risk-based approach. The Associations therefore support Option Two, which provides for a reasonable

time period for verification. The Associations also would support FATF's issuance of best practices guidelines on verification, established with input from the entire spectrum of financial institutions covered by the AML standards.

D. Verification of Existing Accounts

Under section 3.6.1, entitled "Requiring financial institutions to identify all customers, including existing customers," FATF proposes two options for amendment of its standards. Option One would adopt the Basel Committee approach, which suggests that customer identification and verification for existing account holders be based on materiality and risk assessment, and instituted "when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated." Option Two would explicitly require due diligence as to existing customers, but would allow this to be done either within a reasonable time frame or within a fixed period, such as five years after the effective date of the requirement.

In the United States, the proposed rules for section 326 of the USA PATRIOT Act, regarding Customer Identification Programs, require identification and verification of existing customers only if they open a new account or request new authority under an existing account. Given the large numbers of existing accounts maintained at U.S. financial institutions, this limitation is entirely consistent with a risk-based approach. Rather than devote significant resources to verifying every existing account, it is logical to focus on those customers or accounts that exhibit a change in activity or pose enhanced risk, consistent with the approach taken by U.S. regulators in connection with the USA PATRIOT Act. The Associations recommend that FATF adopt a similar risk-based approach. If FATF rejects the risk-based approach on this particular issue, the Associations recommend that financial institutions be given a reasonable time, not less than five years, to complete this resource-intensive task.

E. Simplified Verification of Low Risk Scenarios

In section 3.4 of the Consultation Paper, FATF recognizes the practice in certain jurisdictions of allowing simplified due diligence, i.e., lack of verification, more limited verification, or more limited documentation of the verification, based on a lesser risk of money laundering in particular situations. The Associations agree with FATF's basic premise that, in general, customers should be subject to full identification and verification procedures and that any use of simplified verification should be limited to appropriate cases.

The Associations strongly endorse FATF's options regarding simplified verification for particular categories of customers serviced by the Associations' member firms, such as credit or financial institutions already subject to the FATF standards, large public companies listed on a stock exchange, counter-parties that are publicly known, and regulated entities. The Associations suggest adding, by way of additional examples, pension funds and other accounts that involve little control by the individual investor.

FATF further discusses what would be considered sufficient identification and verification when the customer is itself a credit or financial institution. The Associations strongly endorse the ability of the institution holding the account to verify identity through review of lists of authorized institutions (such as through the website of the applicable supervisory authority) or by confirming with the relevant supervisory authorities that it is a licensed/registered institution. The Associations agree that, in those situations, it would be reasonable for the "primary institution" to rely on the customer institution to identify and conduct due diligence on its own clients, such as where an account is used to pool investment funds from many clients for legitimate purposes, e.g., employer-sponsored retirement accounts, pension funds and mutual funds.

F. Special Verification Procedures for Trusts and Other Corporate Vehicles

Section 4.3 of the Consultation Paper requests comment on how to achieve greater transparency in order to enhance due diligence with respect to trusts. FATF presents a number of options regarding disclosure of information with respect to the trustees, settlors and beneficiaries of trusts. The Associations note only that, given privacy issues with respect to beneficiaries, it should not be necessary to maintain information on beneficiaries who do not control the trust, for whom the risk of money laundering is negligible. This is consistent with the AML regulations relating to trusts in the United States.

Beneficial ownership and control information with respect to other corporate vehicles is addressed in section 4.1 of the Consultation Paper. Here, too, it is the Associations' position that where beneficial ownership of particular corporate vehicles is of limited relevance to AML concerns, i.e., where there is low risk of money laundering, there is little, if any, need to collect and maintain such information. Such corporate vehicles include occupational pension funds, mutual funds and similar types of pooled investments. We commend FATF for also recognizing these exceptions.

II. Intermediaries

A. Reliance on Intermediaries to Perform Identification and Verification Obligations

The Associations strongly endorse FATF's recommendation in section 3.5 to permit financial institutions, in appropriate circumstances, to rely on intermediaries to perform identification and verification obligations. In the securities and related industries, it

is commonplace for financial institutions to maintain accounts for, or transact business with, intermediaries that are trading on behalf of third parties and that not only have performed identification and/or verification procedures, but also are better suited to perform those obligations. In these instances, and if the intermediaries are properly vetted, it is our belief that reliance on such intermediaries not only is appropriate, but essential to conducting business across borders. This approach is consistent with FATF's stated goal of avoiding unnecessary duplication and permitting firms to focus their resources on accounts and relationships that pose higher risks of money laundering.

As FATF recognizes, securities firms frequently deal with domestic and foreign intermediaries that trade and transact other business on behalf of their own customers. The intermediaries are mostly reputable, publicly-traded and highly regulated entities with strong AML programs. FATF cites the practice of brokers placing trades at the request of foreign brokers for the clients of the foreign broker, but there are many other routine transactions in the securities and related industries that involve prior identification and verification of the customer by an intermediary. Other examples include purchases or redemptions of mutual fund shares that are conducted through a broker or other intermediary, brokers clearing trades on behalf of introducing brokers or on behalf of another broker's customers in an omnibus account, brokers executing transactions on behalf of large institutions investing funds for third parties, and prime brokers maintaining accounts for client institutions that conduct transactions on behalf of their own clients or collective investment vehicles, such as hedge funds.

The Associations believe that it is both an unnecessary and an inefficient use of AML resources for the "primary institution" to repeat an intermediary's own due diligence for its clients. The primary institution, in fact, often has a more limited ability to perform identification and verification procedures than the intermediary. Moreover, for many intermediary institutions, there are serious proprietary and privacy concerns in disclosing their own clients to other institutions that are considered competitors.¹³ Therefore, we believe that where the primary institution has satisfied its own due diligence responsibilities with respect to the intermediary, there is no reason for the intermediary to provide documentation relating to its underlying clients to the primary institution. In keeping with the Associations' recommended risk-based approach, the primary institution should devote its resources to investigating clients that deal directly with the institution, rather than indirectly through an intermediary that already has devoted adequate resources towards identification and verification.

The Consultation Paper presents three options for determining the third parties on which primary institutions can rely. The first option permits as intermediary any entity that falls under the definition of "financial institution" contained in section 3.1 of the Consultation Paper. The second option permits as intermediary any third party that is subject to the full range of AML requirements, including the regulation and supervision standards set forth in the Consultation Paper at section 3.8. The last option permits as intermediary any third party that the primary institution is satisfied meets the first four bullet points of the Basel Committee standard for introduced business, and is a member of a class of persons or entities that the jurisdiction determines is acceptable to be third parties.¹⁴

In lieu of adopting one of these options to the exclusion of the others,¹⁵ we suggest that FATF adopt a broad framework that grants flexibility to financial institutions by defining three different categories of intermediary, each requiring its own level of due diligence. Under the first category, if the primary institution confirms the intermediary to be a "financial institution" that is subject to the full range of AML requirements consistent with the FATF standards, the primary institution may rely on that intermediary to perform identification and verification obligations with respect to its customers. For example, a U.S. registered broker-dealer subject to the AML provisions of the USA PATRIOT Act would fall into this category.¹⁶

Under the second category, if the intermediary is a financial institution that is in a FATF member country (or in a jurisdiction that has procedures consistent with the FATF standards) but is not subject to the full range of AML requirements, the primary institution may rely on that intermediary after: (i) conducting appropriate due diligence with respect to the intermediary, in order to satisfy itself that the intermediary is a legitimate, reputable entity that can be relied on with respect to its identification and verification procedures; and (ii) obtaining a representation from the intermediary that certifies that the intermediary has customer identification and verification procedures that are comprehensive and rigorous and meet the concerns of the primary institution.

Once it is determined that the intermediary is in a jurisdiction with standards consistent with FATF, appropriate due diligence by the primary institution with respect to the intermediary could include determining: (i) the depth and duration of the intermediary's relationship with the primary institution; (ii) whether the intermediary is part of a regulated group or is subject to comprehensive consolidated supervision (e.g., whether the intermediary complies with European Union anti-money laundering directives); (iii) whether the intermediary remains in "good standing" within its country of domicile; (iv) the reputation and background of the intermediary, including checking third-party references; (v) whether the intermediary is publicly-held; (vi) whether the particular type of intermediary has been known to raise money laundering concerns; and (vii) background information on the intermediary through researching appropriate databases.¹⁷

The intermediary's representation to the primary institution could contain a description of the identification and verification procedures that the intermediary expects to follow.

If the intermediary does not fall into either of the above categories, the Associations recommend that the primary institution be required to conduct more detailed due diligence with respect to the intermediary, including determining whether the intermediary has implemented identification and verification procedures that are comprehensive and rigorous and meet the concerns of the primary institution. The intermediary need not be subject to a formal supervisory regime, but should, at a minimum, meet the regulatory requirements for its particular jurisdiction, such as proper authorization and registration. After conducting formal due diligence on the intermediary, the primary institution should be able to rely on the intermediary's representations of due diligence. For example, primary institutions should be able to rely on the representations of eligible introducers such as investment advisers who bring their own clients to the primary institution and maintain communication with those clients, to the exclusion of the primary institution. Stronger safeguards could, of course, apply where the intermediary is from a jurisdiction included in FATF's list of Non-Cooperative Countries and Territories ("NCCT").

The Associations recommend that, instead of imposing ultimate responsibility for identification and verification on the primary institution, FATF adopt a more nuanced approach. Thus, the Associations do not endorse the requirement of the Basel Committee that the primary institution collect and review all verification documentation from the intermediary.¹⁸ Review by the primary institution of the verification documentation undermines the purpose of reliance on intermediaries and requires duplication of effort, which is contrary to a risk-based approach. Moreover, in the securities and related industries, the primary institution is often prohibited by the intermediary from obtaining documentation with respect to the latter's customers, as that information is considered proprietary and/or protected by privacy laws.¹⁹

The Associations do, however, propose that where the intermediary resides in an NCCT jurisdiction, or where other factors create enhanced AML risks, the primary institution require the intermediary to re-certify periodically its identification and verification procedures, or request that the intermediary have an independent review of those procedures. The intermediary also should maintain all relevant data and documentation pertaining to each customer's identity, which could, in specific situations, consistent with the requirements of the local jurisdiction, be made available on request of the primary institution, law enforcement agencies or the financial intelligence unit of that jurisdiction.

In other words, in lieu of imposing on the "primary institution" what appears to be a form of "strict liability" even though the primary institution has reasonably relied on an intermediary for identification and verification purposes, the Associations' recommended approach would limit the liability of the primary institution to situations in which it had no reasonable basis for reliance or where it has ignored indicators that such reliance is no longer reasonable.

Lastly, FATF should recognize that there exists a separate category of customer relationship within the securities and related industries, in which two or more financial institutions "share" the account relationship with the customer. These include clearing brokers that clear trades on behalf of introducing brokers, and executing brokers that execute trades for a customer whose trades are settled by a prime broker. By way of example, in one such arrangement, an individual or institutional customer deals directly with both its carrying/clearing broker, which maintains its account and handles its funds, and its executing broker, which executes its transactions. In that situation, each broker has AML obligations with respect to verifying the identity of its customer, as it maintains direct contact with that customer. Another variation of the sharing arrangement, specific to the futures industry, is a "give-up" arrangement, whereby multiple brokers employed by the same customer participate in a transaction on behalf of that customer.

In such circumstances, the financial institutions sharing the customer relationship should be permitted to contractually agree to allocate identification and verification responsibilities among themselves, such as the executing broker contractually relying on the carrying broker (which normally maintains the customer account agreements and related documents and has the more direct relationship with the customer) to verify the identity of the customer. The U.S. Treasury has approved such a contractual allocation of identification and verification responsibilities with respect to shared accounts, including "give-up" arrangements and clearing broker/introducing broker relationships.²⁰ The Associations recommend that, consistent with the flexible, broad framework discussed above,²¹ FATF adopt the same approach in this context.

B. Outsourcing Verification

In section 3.5.2 of the Consultation Paper, entitled "Outsourcing and agency arrangements," FATF recognizes that financial institutions often contract with agents to perform particular financial functions, including identification and verification of customers. FATF queries whether the agent then becomes subject to the same or similar AML and due diligence obligations that apply to the primary institution. FATF suggests that if the primary institution does not receive the relevant documentation and the agent itself is not already subject to due diligence obligations, the primary institution can contractually impose due diligence obligations on the agent.

The Associations endorse reliance in appropriate circumstances on outsourcing of identification and/or verification to agents that are contractually bound to the same due diligence obligations as the primary institution. For example, in the mutual fund context, the transfer agent is the logical entity for implementation of AML procedures, as it maintains shareholder records and accounts and

processes most, if not all, customer transactions. Other potential outsourcers include the fund's investment adviser/sponsor, which could employ its own compliance personnel to verify identity, or the principal underwriter for funds where some or all of transactions flow through the underwriter. Another example in the securities and related industries is a "finder," who might be hired to introduce new clients.

We note that the contractual delegation of due diligence compliance functions has been endorsed by the U.S. Treasury with respect to mutual funds. In the proposed rule for Customer Identification Programs for Mutual Funds and the interim final rule for AML Programs for Mutual Funds, a mutual fund can delegate contractually the implementation and operation of its customer identification and AML programs to another affiliated or unaffiliated service provider, such as a transfer agent.²² Accordingly, we believe appropriate contracting should be endorsed on the international level as well.

III. Correspondent Banking/Payable-Through Accounts

The Associations note that the application in the United States of AML concepts with respect to correspondent accounts has caused confusion for our member institutions, as that term has minimal application in the securities and related industries. Similarly, reference both to correspondent accounts and to payable-through accounts in subsection 3.3.2 of the Consultation Paper, entitled "Correspondent Banking," appears to be limited to accounts established by correspondent banks—normally large, international banks—to provide services to respondent banks—most often foreign banks—that transact business on behalf of third parties. These terms should be limited to the banking industry, and FATF should address any verification issues with respect to collective investment vehicles²³ or other similar arrangements in the securities and related industries under the concept of intermediaries, as discussed above.

IV. Politically Exposed Persons

In section 3.3, entitled "Higher Risk Customers and Transactions," the Consultation Paper notes that there is a growing consensus that international guidance is needed regarding government leaders and public sector officials – collectively referred to as Politically Exposed Persons ("PEPs"). FATF requests comment on "whether an explicit reference to PEPs is necessary or desirable in the revised FATF 40," and, if so, how this could best be done. The three options proposed by FATF are: (1) have a general statement about minimum standards applicable to all account relationships, followed by a reference to the need for higher standards in certain high-risk areas, including correspondent banking and PEPs; (2) supplement the first option with a cross-reference to the Basel Committee CDD Paper; and (3) include concise text in the FATF 40 with respect to PEPs, possibly as part of a new Customer Due Diligence Recommendation.

While we believe any guidance that FATF provides in this context would be of assistance, the Associations strongly recommend that FATF develop an international, publicly available listing of all PEPs, including those who present heightened risks for financial institutions, together with all entities or other investment vehicles known to be associated with such PEPs.

In concept, a "PEP list" would be consistent with FATF's approach in publishing its list of FATF members and identifying NCCTs. Indeed, FATF is in a far better position than an individual financial institution to obtain information about PEPs from its own member countries and other jurisdictions. Like the NCCT list, a PEP list would greatly assist financial institutions in identifying potentially high-risk customers, determining whether to do business with them, and, if so, applying enhanced due diligence procedures to address the associated risks. Thus, instead of financial institutions around the world each having to expend enormous resources merely to determine whether a potential customer is a PEP, they can check the PEP list, conduct their own due diligence, and those that choose to accept the PEP as a customer can focus their resources to applying special procedures and controls to ensure that the customer's accounts are not used for money laundering or other criminal activity.

V. Suspicious Transaction Reporting

With respect to suspicious transaction reporting, in section 3.7, FATF seeks comments on, among other things, the scope and nature of the reporting obligation. The three options proposed by FATF are: (1) leaving it to each country to decide how to implement their reporting requirements; (2) accepting "indirect reporting" (i.e., whereby making a report provides a defense against a money laundering charge); and (3) requiring there to be an explicit obligation to report suspicious transactions, with sanctions for failure to comply.

The Associations believe that, to the extent that a financial institution is subject to an affirmative reporting obligation, it also should be entitled to the benefit of a defense to any money laundering charge. In concept, this is a combination of Options Two and Three, in that if a country requires the filing of suspicious activity reports, it would then give the benefit of such a filing to the institution. Such an approach would be fundamentally fair, as financial institutions acting as "good corporate citizens" by making suspicious transaction reports ought not to be criminally prosecuted. In addition, providing a defense to criminal liability would increase the likelihood that a financial institution will file a suspicious transaction report.

We also recommend that FATF work on establishing a global safe harbor from civil liability for suspicious transaction reporting. Particularly as financial transactions become increasingly global, there is greater likelihood that a financial institution making a suspicious transaction report in one country will be subject to civil suits in other countries (e.g., where the illegal activity takes place in one country, but the individuals affected by that activity or the individuals implicated in the suspicious transaction reside in another jurisdiction). The costs of defending against such lawsuits, particularly in far-off foreign jurisdictions, can be prohibitive, thereby creating a chilling effect on the filing of suspicious transaction reports. Given these circumstances, FATF should develop a system under which a financial institution making a suspicious transaction report in one FATF member country will be afforded a safe harbor from civil liability in all other FATF countries as well.

Lastly, FATF is considering requiring financial institutions to obtain customer identification from a customer at the time it files a suspicious transaction report. The Associations fear that such a requirement, as FATF anticipates, would “tip off” the subjects of the report and therefore be counterproductive to AML measures.

The Associations hope this letter has helped articulate the particular practices and concerns of our member institutions. We would be happy to respond to any further questions that may arise during FATF's process of revising the Forty Recommendations.

Should you have any questions, please contact Betty Santangelo or Sung-Hee Suh of Schulte Roth & Zabel LLP at (212) 756-2000.

Very truly yours,

Futures Industry Association

Investment Company Institute

Securities Industry Association

cc: Daniel Glaser

United States Department of the Treasury

ANNEX A

The Futures Industry Association is a principal spokesperson for the commodity futures and options industry. FIA's regular membership is comprised of approximately 50 of the largest futures commission merchants in the United States, the majority of which are also registered broker-dealers. Among its associate members are representatives from virtually all other segments of the futures industry, both national and international. Reflecting the scope and diversity of its membership, FIA estimates that its members effect more than 80 percent of all customer transactions executed on United States futures exchanges.

The Investment Company Institute is the national association of the American investment company industry. Its membership includes 8,990 open-end investment companies (“mutual funds”), 504 closed-end investment companies and six sponsors of unit investment trusts. Its mutual fund members have assets of about \$6.615 trillion, accounting for approximately 95 percent of total industry assets, and over 88.6 million individual shareholders.

The Securities Industry Association brings together the shared interests of more than 600 securities firms to accomplish common goals. SIA member firms (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. The U.S. securities industry manages the accounts of nearly 93 million investors directly and indirectly through corporate, thrift and pension plans. In the year 2001, the industry generated \$198 billion in U.S. revenue and \$358 billion in global revenues. Securities firms employ approximately 750,000 individuals in the United States.

ENDNOTES

¹ See Annex A for a description of each of the Associations.

² Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 296 (2001).

³ Rule 312, 67 Fed. Reg. 37736 (May 30, 2002) and 67 Fed. Reg. 48348 (July 23, 2002).

⁴ Rule 352, 67 Fed. Reg. 21110 (Apr. 29, 2002) (financial institutions); 67 Fed. Reg. 21114 (Apr. 29, 2002) (money services business); 67 Fed. Reg. 21117 (Apr. 29, 2002) (mutual funds); and 67 Fed. Reg. 21121 (Apr. 29, 2002) (operators of credit card systems).

⁵ Rule 356, 67 Fed. Reg. 44048 (July 1, 2002).

⁶ Rule 326, 67 Fed. Reg. 48306 (July 23, 2002) (broker-dealers); 67 Fed. Reg. 48289 (July 23, 2002) (banks, savings associations and credit unions); 67 Fed. Reg. 48318 (July 23, 2002) (mutual funds); 67 Fed. Reg. 48328 (July 23, 2002) (futures commission merchants and introducing brokers); 67 Fed. Reg. 48299 (July 23, 2002) (banks that do not have a federal functional regulator).

⁷ See Remarks of Carol Sergeant, Managing Director, Financial Services Authority, FSA Money Laundering Conference (July 15, 2002).

⁸ The National Association of Securities Dealers (“NASD”) is a self-regulatory organization whose jurisdiction covers approximately 5,500 brokerage firms, nearly 90,000 branch offices and more than 650,000 registered securities representatives. Among other things, the NASD writes rules governing the activities of member firms, conducts examinations of them and disciplines firms for failure to comply with NASD rules. See www.nasd.com.

⁹ The National Futures Association (“NFA”) is a self-regulatory organization that conducts oversight of the futures industry, including by issuing sales practice rules and financial requirements for its member firms, conducting audits of member firms and disciplining those that are non-compliant. See www.nfa.futures.org.

¹⁰ SIA Anti-Money Laundering Committee, “Preliminary Guidance for Deterring Money Laundering Activity,” available at www.sia.com; Special NASD Notice to Members 02-21, “Anti-Money Laundering” (April 2002), available at www.nasdr.com/pdf-text/0221ntm.pdf; Interpretive Notice, “NFA Compliance Rule 2-9: FCM and IB Anti-Money Laundering Program” (April 23, 2002), available at www.nfa.futures.org/nfaManual/entireManual.asp#45; and Investment Company Institute, “Money Laundering Compliance for Mutual Funds” (May 1999). Note that the ICI compliance paper pre-dates recent AML regulations under the USA PATRIOT Act and therefore is not current in that respect.

¹¹ In addition, due to evolving customer needs, many brokerage accounts are opened electronically as well.

¹² In Annex 1, FATF presents a number of possible measures for managing money laundering risks in non-face-to-face customer relationships. One possible measure would require face-to-face verification for all new customers by either the “primary institution” or the intermediary. Another possible measure would require face-to-face verification of any new customers who fall into certain categories—i.e., those with assets exceeding a specified amount. Adoption of either option would severely burden the securities and related industries and would be considered a significant inconvenience to the law-abiding customer, possibly reducing the amount of business it conducted through brokers. Last, it would absorb a material amount of resources better allocated to higher-risk transactions.

¹³ We note that privacy laws, such as those in the European Union, may preclude or circumscribe the ability of a financial institution to disclose information about its customers. See, e.g., European Data Protection Directive 95/46/EC.

¹⁴ Under the Basel Committee CDD Paper (at p. 9, ¶ 36): (1) the intermediary must comply with the minimum customer due diligence practices identified in the Basel Committee CDD Paper; (2) the customer due diligence procedures of the intermediary must be as rigorous as those which the bank would have conducted itself for the customer; (3) the bank must satisfy itself as to the reliability of the systems put in place by the intermediary to verify the identity of the customer; and (4) the bank must reach agreement with the intermediary that it will be permitted to verify the due diligence undertaken by the intermediary at any stage. For banks only, FATF would also require that the intermediary immediately submit to the bank for review all relevant identification data and other documentation pertaining to the customer’s identity. In addition, under the minimum customer due diligence requirement (the first bullet point), the Basel Committee CDD Paper requires customer verification before a banking relationship is established. See Basel Committee CDD Paper, at p. 6, ¶ 22. The Consultation Paper is unclear as to whether the requirement that customer verification be conducted before a relationship is established would apply only to banks or to all financial institutions.

⁵ Although the three options may have been intended by FATF to be considered in a cumulative fashion, they are set forth in the Consultation Paper as separate and distinct alternatives.

¹⁶ See 67 Fed. Reg. 48318, 48320 n. 14 (July 23, 2002). Under the regulations for the verification procedures of mutual funds, a mutual fund that maintains an omnibus account in a broker-dealer’s name is explicitly exempted from due diligence requirements as to customers comprising the account: “[W]here a mutual fund sells its shares to the public through a broker-dealer and maintains a ‘street name’ or omnibus account in the broker-dealer’s name, the individual purchasers of the fund shares are customers of the broker-dealer, rather than the mutual fund. The mutual fund would not be required to ‘look through’ the broker-dealer to identify and verify the identities of those customers.” Id.

Similarly, under the USA PATRIOT Act, a futures commission merchant or introducing broker maintaining an intermediated account can depend on the intermediary managing the account once it has performed its due diligence as to the intermediary: “With respect to intermediated accounts and accounts for commodity pools and other collective investment vehicles, a futures commission merchant or introducing broker may have little or no information about the identities and transaction activities of the underlying

participants or beneficiaries of such accounts. In most instances, given Treasury's risk-based approach to anti-money laundering programs for financial institutions generally, it is expected that the focus of each futures commission merchant's and introducing broker's [customer identification program] will be the intermediary itself, and not the underlying participants or beneficiaries." 67 Fed. Reg. 48328, 48331 (July 23, 2002).

¹⁷ See, e.g., Proposed Rule for Customer Identification Programs for Futures Commission Merchants and Introducing Brokers, 67 Fed. Reg. 48328, 48331 (July 23, 2002).

¹⁸ Although the options specifically addressing intermediaries appear to limit this requirement to banking institutions (see fn. 14, above), other portions of the FATF Consultation Paper appear to contemplate application of this requirement to all financial institutions. As stated above, we strongly discourage this broader application and request that FATF clarify its intention to limit the requirement.

¹⁹ See fn. 13, above.

²⁰ Proposed Rule for Customer Identification Programs for Futures Commission Merchants and Introducing Brokers, 67 Fed. Reg. 48328, 48331-32 (July 23, 2002); Proposed Rule for Customer Identification Programs for Broker-Dealers, 67 Fed. Reg. 48306, 48308 (July 23, 2002).

²¹ As discussed previously in this section, the framework the Associations propose defines three categories of intermediaries, each requiring its own level of due diligence.

²² 67 Fed. Reg. 48318, 48320 (July 23, 2002); 67 Fed. Reg. 21117, 21119 (Apr. 29, 2002).

²³ A collective investment vehicle is defined under the verification rules of the USA PATRIOT Act as "an entity through which persons combine funds (i.e., cash) or other assets, which are invested and managed by the entity." 67 Fed. Reg. 48328, 48331 n.5 (July 23, 2002).