AMERICAN BANKERS ASSOCIATION

ABASA
ABA SECURITIES ASSOCIATION
An affiliate of the AMERICAN BANKERS ASSOCIATION

1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

World-Class Solutions, Leadership & Advocacy Since 1875

Sarah A. Miller
Senior Vice President
Center for Securities, Trust and Investments
Executive Director & General Counsel
ABA Securities Association
Phone: 202-663-5325
Fax: 202-828-5047
smiller@aba.com

Robert G. Rowe, III
VP/Senior Counsel
Center for Regulatory Compliance
Phone: 202-663-5029
Fax: 202-828-5052
rrowe@aba.com

June 5, 2009

Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: Confidentiality of Suspicious Activity Reports
Docket Number: TREAS-FinCEN-2008-0022

Dear Sir or Madam:

The American Bankers Association (ABA)[1] and the ABA Securities Association (ABASA)[2] appreciate the opportunity to comment on the Financial Crimes Enforcement Network (FinCEN) proposal to update rules for Suspicious Activity Reports (SARs) and to issue new guidance on sharing SARs across a financial enterprise. The regulatory update is designed to reinforce SAR confidentiality while the accompanying guidance is proposed to allow companies to share SARs within the corporate structure to facilitate and promote greater enterprise-wide risk management.

ABA and ABASA commend FinCEN for taking steps to protect the confidentiality of SARs and SAR information and to re-emphasize the sanctity of the SAR process. We support FinCEN's separation of SAR disclosure from SAR sharing as a viable distinction that recognizes the important policy and legal differences between protecting SAR information from being revealed to subjects of suspicious activity reporting versus enabling financial institutions to share SAR information across the corporate enterprise to manage better compliance with suspicious activity detection and reporting obligations. This approach appears to build on an initiative taken in response to strong recommendations of ABA and the industry whereby FinCEN and the banking regulators concluded in early 2006 that it was appropriate to share information with the bank or holding company head office or other controlling entities, no matter where located.[3]

---

[1] ABA brings together banks of all sizes and charters into one association. ABA works to enhance the competitiveness of the nation's banking industry and strengthen America's economy and communities. Its members – the majority of which are banks with less than $125 million in assets – represent over 95 percent of the industry's $14 trillion in assets and employ over 2 million men and women.

[2] ABASA is a separately chartered affiliate of the American Bankers Association representing those holding company members of the ABA actively engaged in capital markets, investment banking, and broker-dealer activities.

[3] The *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies* was issued over three years ago on January 20, 2006. The guidance, a joint effort between FinCEN and the four federal bank regulatory agencies, allows a financial institution to share SARs with a head office or controlling company, no matter where located, provided there is a written confidentiality agreement with the head office or controlling company. The sharing of SARs is designed to allow the head office or controlling company to carry out its supervisory responsibilities and to allow the corporation to design an efficient and effective enterprise wide risk management program.

At that time, it was anticipated that additional guidance would soon be forthcoming to facilitate the ability of corporations to manage risk and better detect suspicious activities by allowing them to share information internally within the confines of appropriate and reasonable corporate controls. Unfortunately, the proposed guidance falls short of this policy promise by imposing unnecessary restrictions on sharing among affiliates within the legitimate enterprise-wide compliance structure that includes the bank or financial institution. Rather than extend the geographically neutral position of the 2006 guidance, the current proposed guidance creates an unwarranted demarcation between affiliated operations located in the United States and those located outside the United States.[4] The proposal also places other limitations on the manner of sharing within the scope of the legitimate enterprise compliance program, limitations that needlessly restrict internal information exchange and impair suspicious activity risk management and reporting. Accordingly, ABA and ABASA oppose proposed guidance that: (a) restricts SAR sharing to affiliates subject to a SAR requirement rule issued by FinCEN or one of the federal banking regulators; (b) imposes new requirements to have a written confidentiality agreement with an affiliate to ensure SAR confidentiality despite the existence. of other suitable controls; and (c) applies new barriers in the chain of sharing among affiliates Instead, ABA and ABASA urge FinCEN to facilitate SAR sharing with affiliates which will protect confidentiality while producing more robust information for law enforcement.

We agree with FinCEN that the critical element in developing the new guidance is the need to share confidential information in a way that carries out the aims and goals of the Bank Secrecy Act (BSA). ABA and ABASA also firmly believe that a more flexible approach to sharing within the comprehensive controls afforded by the overall enterprise's compliance program is both appropriate and an important step to achieving this goal. The ability to share SARs within the enterprise provides critical information needed by the various components of a financial institution to identify, detect and report suspicious activities. Conversely, inability to share that information can only undermine robust compliance and the ability to provide the information law enforcement needs to combat money laundering and terrorist financing. The 2006 *Guidance* allowed SARs to be shared without geographical limits and there has been no indication that this has been either unsafe or unsound. Based on the experience of over three years, it would be entirely appropriate to extend that sharing to affiliates without geographical limitation. And finally, ABA and ABASA urge FinCEN not to place domestic financial institutions at a competitive disadvantage with their foreign counterparts. As has often been noted, criminal elements migrate to financial institutions with the weakest controls, and handicapping financial institutions' ability to share SARs becomes a weakness that criminal elements might seek to exploit.

Clearly, FinCEN agrees that artificial barriers to SAR sharing are an unnecessary impediment. Only this month, FinCEN Director James H. Freis, Jr., confirmed his desire to remove these impediments when he stated that, "[t]he ultimate aim is to allow SAR information to be shared between all affiliates of a global corporate

[4] The guidance as proposed would also handicap sharing with domestic affiliates, such as mortgage brokers, not subject to comparable SAR compliance regulations.

entity no matter where they are around the world."[5] While we agree with the Director and strongly support his goal, we disagree with his premise that the proposal is a good first step. Instead, as we recommend in our comments, additional flexibility should be adopted now to remove these impediments and protect financial markets. There is no good reason to delay the ability of enterprises to share SARs internally as would be the case by adopting the guidance as proposed. Further delay only prevents financial institutions from providing law enforcement with the best information.

SAR Confidentiality - Background

For a variety of policy reasons articulated in the proposal,[6] the BSA prohibits a financial institution, its officers, directors, employees or agents from notifying any person involved in a suspicious transaction that the transaction was reported. Recognizing the importance of maintaining the confidentiality of SARs, the USA PATRIOT Act strengthened SAR confidentiality by adding a prohibition that bars officers or employees of both federal or state governments as well as local, tribal, or territorial governments from disclosing to any person involved in a suspicious transaction that that transaction was reported, other than as necessary to fulfill their official duties.[7] And finally, to encourage reports of possible suspicious activities, the law includes a safe harbor from liability for those who report suspicious activities in good faith. There is nothing in the statutory mandate that restricts sharing of SAR information within a financial institution, among its offices, affiliates, employees or agents.

The Proposed Rule and Guidance

FinCEN approaches the proposed clarification of SAR confidentiality by devising a general rule of confidentiality and non-disclosure accompanied by regulatory rules of construction that are further interpreted by proposed guidance that extends existing guidance pronouncements.

The proposed rule states that a SAR, and any information that would reveal the existence of a SAR, are confidential and may not be disclosed except as described by the further provisions of the rule.

The rule imposes a duty of non-disclosure on financial institutions and government authorities. FinCEN then proposes narrow exceptions to the financial institution duty of non-disclosure through rules of construction incorporated into the regulations.[8]

The proposed rules of construction allow limited disclosure or sharing of a SAR or SAR information under the following circumstances:

---

[5] Message from the Director: Egmont Plenary, June 4, 2009, http://www.fincen.gov/whatsnew/html/20090604.html.
[6] See, e.g., *Federal Register,* vol. 74, no. 44, March 9, 2009, p. 10150.
[7] USA PATRIOT Act section 351, 31. U.S.C. 5318(g)(2)(A)(ii).
[8] While ABA and ABASA believe it would be simpler and cleaner to apply well-defined exceptions rather than create rules of construction, we see no reason to oppose this unusual regulatory construct.

- A SAR may be disclosed to FinCEN, any federal, state or local law enforcement agency or any federal or state regulatory agency that examines the financial institution for compliance;
- To minimize confusion, the proposal clarifies that even though the SAR may not be disclosed, the underlying facts or transactions and documents that serve as the basis for the SAR may be disclosed (not including prior SARs that may be taken into account in filing a later SAR);
- In addition, a SAR can be ***shared*** within the bank's corporate structure for purposes consistent with Title II of the BSA.

Finally, FinCEN proposes to continue existing guidance from 2006 with respect to sharing SARs with controlling entities and to add new guidance allowing sharing with affiliates that are subject to SAR regulations under U. S. law.

Comments on the Proposed Rule and Guidance

The scope of SAR confidentiality must include information that would reveal the existence of a SAR or that was used to support the filing or non-filing of a SAR.

ABA and ABASA concur in FinCEN's delineation of the scope of SAR confidentiality as being not only the SAR itself, but also information that would reveal the existence of a SAR. We agree with FinCEN that there are numerous reasons for this extension as recited in the Supplementary Information to the proposal.[9]

For similar reasons, we also urge FinCEN to formally recognize established precedent that further embraces all material contained in the reporting institution's designated files supporting its decision on filing a SAR as part of the confidentiality obligation. The investigative use and assembly of such material as part of the suspicious activity detection, determination and reporting process warrant being embraced within the SAR confidentiality parameters. As FinCEN notes in the proposed rules of construction, the original records produced *in the ordinary course of business* do not fall within such confidentiality parameters.[10] Although frequently based on documents created in the ordinary course of business, records created as part of the SAR investigation and reporting process are distinct—including those investigatory materials leading to a decision not to file a SAR – and should ***not*** be deemed records produced in the ordinary course. Records produced or used to produce SARs or investigate suspicious activities should be deemed part of the SAR process and therefore confidential. There is judicial precedent to support this approach[11] and we urge FinCEN to incorporate this protection clearly in the final rule.

[9] *See* 74 *Federal Register* at 10150.
[10] See 74 *Federal Register* at 10151. See also, *Cotton v. Private Bank and Trust Co.,* 235 F. Supp. 809, 815 (N.D. Ill. 2002).
[11] See ***Union Bank of California, N.A. v. Superior Court (Grafton Partners, L.P.) (2005) , Cal.App.4th,*** information and analysis gathered and segregated as part of the decision-making process to determine whether ***or not*** to file a SAR is also within the purview of protected confidentiality.

SARs should be treated confidentially to prevent disclosure outside the financial organization structure.

The statutory premise for FinCEN's proposal on treating SAR information confidentially is predicated on the original Bank Secrecy Act provision that financial institutions, their officers, directors, employees or agents are prohibited from notifying any person involved in a suspicious transaction that the transaction was reported. Although there is no broader legislative directive with respect to financial institution handling of SAR information, ABA and ABASA concur that "[p]ermitting disclosure to *any* outside party may make it likely that SAR information would be disclosed to a person involved in a transaction,"[12] with its attendant adverse consequences for law enforcement, for institution security, and for the reliable functioning of the suspicious activity reporting system.

The key then is determining what constitutes an outside party. As the law makes clear, this does not cover the financial institutions themselves or their component staffs, whether officers, directors, employees or agents. Neither does it include government entities with law enforcement or supervisory authority.

Sharing SARs within a financial enterprise's BSA compliance structure should be encouraged to promote compliance with the BSA and to provide appropriate information for law enforcement.

FinCEN's regulatory proposal makes an important distinction between SAR disclosure to outside parties and ***sharing*** of confidential SAR information within the financial institution's "corporate organization structure for purposes consistent with Title II of the Bank Secrecy Act…." ABA and ABASA agree with the validity and value of this distinction, because it adheres closely to the statutory predicate for SAR confidentiality—not disclosing the information to those conducting suspicious transactions to prevent them from becoming aware their conduct has been reported. ***Sharing*** SAR information within the financial institution's organization structure, on the other hand, recognizes that the ability effectively to detect, identify and report suspicious activity requires the assembly of varied sources of transactional information from the institution's records along with staff observations to provide sufficient context to determine whether the conduct departs sufficiently from legitimate business activity to warrant reporting. In FinCEN's words, such sharing is likely "to facilitate more effective enterprise-wide monitoring."[13]

Since the Federal Financial Institutions Examination Council (FFIEC) published the *Bank Secrecy Act/Anti-Money Laundering Examination Manual* in 2005, there has been an increasing focus on enterprise-wide risk management (ERM). Financial institutions have been strongly encouraged to develop risk-management systems that work across the enterprise and are not confined or limited to individual entities within the corporate umbrella. The current manual, published in 2007, stresses the need for companies to develop ERM programs. For example, the manual states that, "When evaluating the enterprise-wide BSA/AML compliance program for adequacy, the examiner should determine

[12] 74 *Federal Register* at 10151.
[13] 74 *Federal Register* at 10151.

reporting lines and how each subsidiary fits into the overall enterprise-wide compliance structure. This should include an assessment of how clearly roles and responsibilities are communicated across the organization. The examiners should address how effectively the holding company or lead financial institution monitors the compliance throughout the organization with the enterprise-wide BSA/AML compliance program, including how well the enterprise-wide system captures relevant data from the subsidiaries."[14] While the manual clearly underlines the then-applicable interpretation of the SAR confidentiality requirements to state that information may not be shared with affiliates, it goes on to state that "in order to manage risks across the organization, banks may disclose to entities within their organization the underlying information supporting a SAR filing."[15]

As stressed by the Board of Governors of the Federal Reserve, "a firmwide compliance function that plays a key role in managing and overseeing compliance risk while promoting a strong culture of compliance across the organization is particularly important for large, complex organizations that have a number of separate business lines and legal entities that must comply with a wide range of applicable rules and standards."[16] The Board goes on to point out that this "need for a firm-wide approach to compliance risk management at larger, more complex banking organizations is well demonstrated in areas such as anti-money laundering…"[17] In order to meet these requirements, the ability of a large, complex banking organization to share information – including SARs – is extremely important.

As noted, the proposal recognizes that, consistent with ERM and the BSA, internal sharing of SARs is appropriate. Therefore, it is critical to understand what entities are encompassed by the phrase "corporate organization structure for purposes consistent with Title II of the Bank Secrecy Act." First, as described in the Supplementary Information, permissible sharing includes sharing by depository institutions, broker-dealers, mutual funds, futures commission merchants, and introducing brokers in commodities or any officer, director, employee or agent of these institutions or among those institutions or individuals within the corporate organization structure. This description, like the statutory language upon which it is built, makes no distinction about where the institution has its offices or conducts its business or where its officers, directors, employees or agents work or reside. In other words, this regulatory structure is geographically neutral.

Second, the proposed guidance for depository institutions[18] addresses only affiliates within the corporate organizational structure and does not address **or limit** sharing within or among divisions or offices of the reporting financial institution.[19] This position is legally sound and represents wise policy. For example, global financial institutions set up information systems to enable employees to access applications such as case management systems from a

[14] FFIEC BSA/AML Examination Manual, 2007, p. 151.
[15] FFIEC BSA/AML Examination Manual, 2007, p. 152.
[16] Federal Reserve Supervisory Letter SR 08-8 issued October 16, 2008, p.1.
[17] *Ibid*, p. 3.
[18] *See* 74 Fed. Reg. 10158 et seq., March 9, 2009
[19] For these purposes, we are referring to departments or divisions within the corporation, not branches.

variety of locations, even outside of the United States. Global business requires global travel and remote access. To suggest that an employee of a financial institution working from a facility outside of the United States should be precluded from accessing SAR systems while logging in from a non-U.S. facility of the financial institution is wholly unworkable and would impede enterprise-wide program management when viewed as part of the administration of the institution's global AML policy and would inhibit achievement of the purposes of an effective AML program in deterring financial crime.

Consequently, when engaged in the financial enterprise's comprehensive BSA compliance program that is expected under the implementing regulations of Title II of the BSA, all officers, directors, employees and agents of such BSA-obligated institutions must be permitted to share confidential SAR information, no matter where they work or reside and independent of any cross-border limitations. ABA and ABASA strongly support this approach and believe it is a necessary element to the ability of a company to comply with the BSA.

As we read the regulatory proposal and its associated proposed guidance, it enables banks to take advantage of the efficiencies of "global sourcing." "Global sourcing" refers to the practice of conducting bank or financial institution operations at a location other than the "home" jurisdiction. For United States financial institutions, global sourcing includes the performance of certain functions **by employees or agents at locations outside the United States.** Examples may include the operation of call centers or information technology processing centers at offices in Ireland or India. Regardless of their location, the employees are employees of the financial institution chartered in the United States and performing specified functions under the obligations imposed by U.S. law and subject to the internal controls of the institution's comprehensive, enterprise-wide BSA compliance program. Furthermore, when a company is hired to perform a function that would otherwise be performed by the financial institution, that company becomes an agent of the financial institution and as such should be able to undertake all the necessary steps to detect, investigate and report suspicious activity on the part of the principal financial institution. Increasingly, the need to rely on the expertise of these third parties is needed to comply with increasingly complex regulations.

Consistent with the increasing globalization of other sectors, a variety of anti-money laundering functions such as customer due diligence and case management information technology support are sourced globally. For global financial institutions it makes sense economically and operationally to centralize these functions in one jurisdiction (not necessarily the United States) while using local resources and expertise. A corporation undertakes appropriate due diligence and implements internal controls to manage any inherent risks when it determines where to locate these operations. Artificial geographic limits undermine a financial institution's ability to manage risk effectively and comply with anti-money laundering obligations.

Accordingly, we support FinCEN's regulatory proposal to the extent it includes within the corporate organization structure of permissible sharing among all employees or agents engaged by the U.S. chartered reporting financial institution. This can be particularly important in those instances when a financial

institution relies on other subsidiaries to perform compliance functions as the part of an effective enterprise-wide risk management program or where employees serve dual roles within the corporate structure and report to one or more subsidiaries. ABA and ABASA strongly encourage FinCEN to clearly incorporate this approach clearly in the final rule as a step to facilitating the detection and reporting of information in the most efficient way to provide the best information to help the financial institution and law enforcement combat money laundering and terrorist financing.

Sharing SARs with holding companies or other controlling entities as part of an enterprise-wide BSA compliance program is not and should not be a prohibited disclosure.

FinCEN's proposed guidance expressly continues in place the existing guidance issued in January 2006 covering holding companies of reporting financial institutions or their other controlling entities without regard to the location of such parent companies. As FinCEN notes, the "sharing of a SAR or, more broadly, any information that would reveal the existence of a SAR, with a head office or controlling company (including those located overseas) promotes compliance with the applicable requirements of the BSA by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a depository institution's compliance with applicable laws and regulations.[20]"

ABA and ABASA heartily support this guidance and believe that it represents a sound policy basis for extending the sharing of SARs among other types of affiliates with one caveat, i.e., the insistence on written confidentiality agreements is unnecessary in the face of appropriate internal controls protecting SAR confidentiality as part of the enterprise-wide AML/CFT (anti-money laundering/countering the financing of terrorism) compliance program. FinCEN has made no showing that written confidentiality agreements should be compelled in place of other effective internal controls.

Sharing SARs among affiliates as part of an enterprise-wide BSA compliance program should be encouraged.

As part of its proposed guidance for depository institutions, FinCEN approves the sharing of SARs among affiliates "provided the affiliate is subject to a SAR regulation" under the U.S. Code of Federal Regulations. FinCEN reasons that the sharing of SARs with such affiliates facilitates the identification of suspicious transactions taking place through the depository institution's affiliates that are subject to a SAR rule." Because FinCEN differentiates holding companies or parent controlling entities from affiliates in its definition under the proposed guidance, the qualification of being subject to a SAR regulation does not apply to bank sharing with its holding company or controlling entities.[21]

[20] 74 *Federal Register* at 10161.
[21] But see our recommendation for redefining "affiliate" to include controlling entities to better consolidate appropriate sharing standards, and to remove as to controlling entities or affiliates any requirement to be subject to a SAR regulation.

While we agree that at a minimum banks should be permitted to share confidential SAR information with affiliates subject to a SAR regulation, we object to FinCEN drawing the line at such types of affiliates and not extending this ability to share with all affiliates functioning within and under the corporate organization's BSA compliance program. ABA and ABASA believe that as long as an enterprise-wide BSA compliance program includes appropriate controls for maintaining SAR confidentiality, any affiliate governed by the enterprise-wide compliance program should be eligible for permissible SAR sharing without further conditions. The goal is an effective and efficient process within the enterprise to detect, identify and report suspicious activities. Proposing to distinguish affiliates artificially prevents this.

Domestic Affiliates. Domestic affiliates not directly subject to SAR rules but that are subject to the corporate organization's enterprise-wide BSA compliance requirements can play an important role in enabling SAR filing affiliates to detect and evaluate financial crime by affording the reporting entity useful information and relevant context for the transaction in question. For example, in March 2009, FinCEN issued the fourth in a series of white papers that detailed the interrelated nature of criminal enterprises that include mortgage fraud.[22] The white paper clearly recognizes that fraudulent enterprises can cross boundaries within a financial institution. At the time the report was issued, FinCEN Director James H. Freis, Jr. stated that, "[t]he interconnected nature of suspicious activity across multiple financial sectors covered by FinCEN's Bank Secrecy Act regulations underscores the immense value of combining insights from the different sectors for the purpose of detecting and thwarting criminal activity."[23]

Based on that premise, if it is logical to combine data across sectors, it certainly should follow that a company is better positioned to address fraud if it can combine insights internally. However, under the artificial constraints that would be in effect under the proposal, a bank would not be able to share SAR information with a separate mortgage broker affiliate. Similarly, a securities firm would not be able to share SAR information with a separate transfer agent affiliate. As long as these domestic affiliates are subject to the same controls and are part of the enterprise's overall BSA compliance program, preventing the sharing of data handicaps the identification, detection and deterrence of criminal activity.

Foreign Affiliates. Foreign affiliates not directly subject to United States SAR rules, but that are subject to the enterprise-wide AML/CFT compliance program, can also play an important role in enabling SAR filing affiliates to detect and evaluate financial crime, especially involving cross-border transactions or foreign customers. The geographic location of such affiliates should not be a bar to SAR sharing.

The interagency guidance issued by FinCEN and the federal banking regulators in January 20, 2006, concluded that a U.S. branch or agency of a foreign bank may disclose a SAR to its head or controlling office within or outside of the United

---

[22] *Mortgage Loan Fraud Connections with Other Financial Crime,* March 2009, *http://www.fincen.gov/news_room/rp/files/mortgage_fraud.pdf.*

[23] FinCEN Press Release, F*inCEN Report Shows Connection With Mortgage Fraud and Other Financial Crime*, March 16, 2009, http://www.fincen.gov/news_room/nr/pdf/20090316.pdf.

States.[24] While the focus of that guidance was on SAR sharing with controlling entities, it was predicated on the conclusion that geography is not a legal barrier to SAR sharing. Thus, the legal and policy underpinnings of this proposed guidance argue for its extension to permit access to SAR systems—as the bank deems necessary pursuant to its administration of an enterprise-wide BSA compliance program—throughout the related entities of an organization, regardless of geographic boundaries.

The compartmentalization of sharing of SARs and information that would reveal the existence of a SAR along financial corporate lines is not consistent with how financial holding companies manage complex businesses. In other words, **corporate form should not trump BSA function.** Although lines of business may cross corporate entities in various jurisdictions, individuals must have access to information from all those entities in order to do their specified jobs effectively and to ensure the safe and sound operations of the enterprise. That information may include SAR information that comes from another company within the enterprise located in another country. Even in a monolithic structure, not all managers reside in the United States, and it is not unusual for a manager to work outside the United States while managing business lines and staff within the United States. Just as a headquarters or controlling entity must have access to SAR information to supervise operations, as acknowledged in the 2006 guidance, it is even more practically vital that the manager receive information about the risk of her or his business.

Maintenance of an enterprise-wide BSA program requires the secure sharing of SARs throughout the organization—not only upward to head offices, but laterally with branches, administrative offices and affiliates at home or abroad. Restricting this exchange of information will seriously impede efforts to manage potential risks, especially money laundering or terrorist financing. It also becomes a barrier to the ability of affiliates within an organization to detect and report additional suspicious activity based on what has already been identified and reported under other regimes. As pointed out by FinCEN Director Freis, "[w]e have inadvertently created a system that has led to inefficiencies and duplications of cost because institutions have to create separate systems of collecting SARs that are walled off between different entities even though they are part of the same corporate family. Those impediments are preventing the institution from protecting itself and ultimately, financial markets."[25]

The limitation of cross-border SAR sharing to controlling companies is an artificial restriction that undermines the need for all *responsible* parts of an organization to have knowledge of enterprise-wide Bank Secrecy Act/anti-money laundering risks and, as needed, to have SAR access to fulfill their compliance and risk management responsibilities. We cannot stress strongly enough that when the 2006 *Guidance* on sharing with headquarters and controlling entities was adopted, the ability to share SARs cross-border was accepted. Nothing has been suggested that this experiment was a failure or that appropriate controls cannot or are not in place to address any potential risks.

---

[24] *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies* (Jan. 20, 2006). *See also* Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities (Jan. 20, 2006).
[25] Message from the Director: Egmont Plenary, June 4, 2009.

In a footnote to the proposed guidance,[26] FinCEN states that "because foreign branches of U. S. banks are regarded as foreign banks for purposes of the BSA, under this guidance, they are 'affiliates' that are not subject to a SAR regulation. Accordingly, a U. S. bank that has filed a SAR may not share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches." Unlike global sourcing, where the employees and agents generally do not provide banking services but support operations by allowing financial institutions to take advantage of the efficiencies of the global economy, subject to the internal controls of the financial institution, foreign branches have been historically regarded as separate entities. Still, foreign branches are part of the larger enterprise subject to the same internal controls, and so, ABA and ABASA strongly encourage FinCEN to continue to evaluate the need for instituting this firewall and restricting communications. As noted in the FFIEC BSA/AML Examination Manual at page 156, "banks are expected to have policies, procedures, and processes at the foreign office to protect against risks of money laundering and terrorist financing." As part of an integrated whole, it is important and logical to communicate and share information between all branches of the enterprise. While this does not and should not create a separate SAR filing obligation for the foreign branch, the ability to share information and to alert the foreign branch easily to possible fraud, money laundering or other risks, is integral to the ability of the foreign branch to provide data and background information that helps the enterprise detect and report suspicious transactions. As noted by FinCEN Director Freis, "the global interconnections of the financial markets are beyond dispute."[27] Director Freis went on to point out that, "[c]riminals and terrorists do not respect the law; they certainly do not respect national borders. They will seek to exploit the weakest link to move and launder money through any means of financial intermediation."[28] ABA and ABASA agree wholeheartedly with the Director's assessment and firmly believe that SAR sharing under appropriate enterprise-wide internal controls is consistent with the purposes of the BSA and is the best and most efficient means to accomplish this goal, including sharing with foreign branches and other foreign affiliates.

Another very serious problem with restricting the ability to share SARs and SAR data within an enterprise structure that crosses borders is that it delays posting and sharing of the information. As criminals become increasingly savvy and nimble, the ability for companies to share data that might lead to the detection of fraud is critically important. Expedited timing can often mean the difference between avoiding a loss and catching a criminal or incurring substantial losses and letting a criminal – or financial terrorist – elude capture. The inability to share and communicate also means that the information provided to law enforcement through SAR filings will be less informative and therefore less useful to law enforcement efforts to combat money laundering, terrorist financing and other criminal activities.

Finally, excluding foreign affiliates that are part of an enterprise-wide AML/CFT compliance structure also seems to contradict what FinCEN has articulated in

[26] 74 *Federal Register* 10161, footnote 8.
[27] Prepared Remarks of James H. Freis, Jr., Director, Financial Crimes Enforcement Center, 10th Annual Anti-Money Laundering and Financing Terrorism International Seminar, Acapulco, Mexico, October 9, 2008, p. 2.
[28] Ibid.

other venues. For example, in a speech last year FinCEN Director Freis stated, "I would like to emphasize that the U.S. Government very much favors a multinational approach."[29] He went on to cite testimony by United States Treasury Under Secretary for Terrorism and Financial Intelligence Stuart Levey, delivered only days earlier in a Congressional hearing: "Given the global nature of the financial system, focusing only on the U.S. financial system and its AML/CFT regime is not sufficient. Safeguarding the U.S. financial system requires global solutions and effective action by financial centers throughout the world. We work toward this objective through multilateral bodies that set and seek to ensure global compliance with strong international standards."[30] In other words, it is important to trust the AML/CFT regimes in other jurisdictions, including their ability to protect SARs and SAR data.[31]

Consequently, we strongly recommend that the types of affiliates qualified for sharing within a BSA compliance program be extended under the proposed guidance to include all domestic affiliates, even those that are not directly subject to a SAR regulation, and to foreign affiliates as long as the affiliates in question are covered by the controls of an enterprise-wide BSA compliance program that includes reporting financial institutions. The key to SAR sharing within the corporate organization structure is that SAR confidentiality is protected by the internal controls included in the enterprise-wide compliance program. FinCEN should not allow corporate **form** to interfere with a properly organized risk-based BSA compliance **function**.

It is very important to recognize that our alternative would not *compel* sharing among affiliates, but rather would *enable* sharing where the corporate organizational structure has carefully established an enterprise-wide BSA compliance program that covers the particular affiliates intended to be within the scope of permissible sharing of confidential SAR information. In other words, sharing would not be mandatory but would be permissible as part of and consistent with an overall AML/CFT compliance program. Corporations are sensitive to and well-positioned to control risks, including reputational risk. A financial holding company will not share information with an affiliate unless appropriate controls can be implemented and maintained.

Comments on Additional Proposed Restrictions to Sharing

Building upon the predicate that SAR sharing should be coterminous with the scope of the enterprise-wide BSA compliance program, it follows that imposing additional restrictions beyond the risk-based internal controls of the compliance program is not warranted. Therefore, ABA and ABASA set forth our objections to

---

[29] Prepared remarks of James H. Freis, Jr., FinCEN Director, "*Global Markets and Global Vulnerabilities: Fighting Transnational Crime Through Financial Intelligence*," delivered at the Academic Session on "Global Initiatives To Avoid The Mis (Use) Of The Financial System For Illegal Purposes" of the Committee On International Monetary Law Of The International Law Association (MOCOMILA), Salamanca, Spain, April 25, 2008.

[30] See http://www.treas.gov/press/releases/hp898.htm

[31] This is not to suggest that all countries have comparable AML/CFT regimes and that SAR sharing should be shared in all instances. Rather, it is to suggest that SAR sharing should not be artificially limited to domestic entities under the purview of the United States BSA requirements. Just as a financial institution is charged with controlling risks, it should have the flexibility to ascertain when and where SARs and SAR data should and can be shared with affiliates in other jurisdictions.

several additional limits to the SAR sharing process contained in the proposed guidance that unduly impair and burden sound compliance.

Definition of Affiliate. As with so many regulations, the definition of an affiliate will be critical. The definition that FinCEN intends to use is that "an 'affiliate' is effectively defined as a company under common control with, or a subsidiary of, the depository institution."[32] While we agree with this definition, ABA and ABASA suggest it be included in the body of the final guidance to avoid confusion. In the preamble to the proposal, FinCEN stresses that the definition "does not include holding companies because sharing with these entities is already addressed in the 2006 Guidance." Since many corporations that operate around the globe will be developing procedures that rely on both the 2006 Guidance on sharing with the Head Office as well as this guidance on sharing with an affiliate as integral parts of a suspicious activity and risk management program, we urge that the two be integrated to reflect corporate reality. Moreover, since the two pieces of guidance will operate as integral parts of a whole, the definition of affiliate should incorporate the 2006 Guidance scope of controlling entities, as well as its geographic neutrality.

An Affiliate Should Be Allowed to Pass Along a SAR. The proposal would add another restriction to prevent a financial institution that receives a SAR from an affiliate from further sharing that SAR. This is another artificial limitation that will only create confusion and unnecessary burdens and that should be stricken from the final guidance. For example, to comply with this restriction, a company will have to develop a mechanism to segregate SARs it has filed from SARs it receives from affiliates. For a large company with multiple affiliates, that creates an almost impossible compliance administrative burden. It also becomes a handicap to internal communication that will make it difficult to identify and manage risk. This part of the proposal is micro-management and an unnecessary imposition on the institution's risk management judgment. Deference is deserved and should be given to the enterprise-wide compliance program to manage properly access to SAR information that will balance its confidentiality with its probative value in the detection and reporting process.

Written Confidentiality Agreements. Another requirement in the proposal is that, to share SARs or SAR data a financial institution should have written confidentiality agreements with its affiliates. We contend that this step is an unnecessary element and should be eliminated. Confidentiality agreements are not an ideal solution for a complex financial services enterprise. Generally, if a company has appropriate processes and procedures to ensure that the confidentiality of SARs and SAR data is maintained, that should be sufficient.

The fundamental concern is protecting the confidentiality of the SAR. Internal policies and procedures can accomplish that without the need for separate confidentiality agreements between affiliates within the corporate structure. Written confidentiality agreements may be appropriate for unrelated independent organizations but are not necessary for affiliates within the same organization. Instead, it would be simpler and more closely aligned to existing guidance on AML/CFT risk management to require that the financial holding company

[32] *Federal Register,* vol. 74, no. 44, March 9, 2009, p. 10159, footnote 10.

establish policies requiring all employees of the enterprise to maintain the confidentiality of SARs and information that would reveal the existence of a SAR. Affected companies within the enterprise can implement procedures and practices to assure that the policy is followed. It also would be useful to acknowledge that an employee of a subsidiary of a financial holding company can act as agent on behalf of the financial holding company to receive SARs or information that would reveal the existence of a SAR. This would be simple, efficient, effective and in accordance with the established regulatory approach.

Fundamentally, the problems that result from artificially restricting information sharing with affiliates handicap the ability of a corporation to manage risk effectively and efficiently across the enterprise. In other words, the restrictions in the proposed guidance not only restrict the ability of a company to have a full and robust ERM program but the ability to detect and deter fraud and other criminal enterprises. And those same restrictions mean a company will be less capable of providing the very information needed by law enforcement to stop criminal activities. While it may be a tired cliché, the restriction on affiliate sharing is akin to the concept of asking a man to fight with one hand tied behind his back.

Concerns About Disclosures in Foreign Jurisdictions Can Be Mitigated.

FinCEN solicits input on how to handle the possibility of forced disclosure in foreign jurisdictions. ABA and ABASA assert that such possibilities occur infrequently, if at all. The 2006 guidance states, "[t]he sharing of a Suspicious Activity Report with a non-U.S. entity raises additional concerns about the ability of the foreign entity to protect the Suspicious Activity Report in light of possible requests for disclosure abroad that may be subject to foreign law."[33] However, despite more than three years of experience, FinCEN offers no cases or statistics detailing real experiences with such incursive requests. Certainly FinCEN's extension of the 2006 guidance without remarking about the incidence of unwanted foreign disclosure suggests that foreign disclosure concerns are practically immaterial. There is certainly no reason to believe that their incidence will be any greater or more practically problematic due to foreign affiliate sharing.

We agree that financial institutions should take appropriate steps to protect and preserve the confidentiality of SAR information across the institution but believe that any issues arising from such requests should be addressed by the protocols arising under the Egmont Group and the common principles for implementing SAR regimes by the FATF jurisdictions.

Since 2001, the international exchange of sensitive information relating to suspected money laundering and terrorist financing has been governed by *The Egmont Group Principles for Information Exchange* (the Principles).[34] The Principles seek to facilitate information exchange and to overcome the obstacles preventing cross-border information sharing between financial information units

[33] *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies,* January 20, 2006, p. 2.
[34] The Egmont Group, *Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases,* June 13, 2001, http://www.egmontgroup.org/files/library_egmont_docs/princ_info_exchange.pdf.

(FIUs), but they also establish rules governing conditions for the exchange of information, permitted uses, and confidentiality/protection of privacy.

Egmont Group members, including FinCEN, have agreed that the information exchanged between FIUs may be used only for the specific purpose for which the information was sought or provided, and the requesting FIU may not transfer information to a third party or make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information. Thus, there exists an established process for protecting sensitive information that can be used to address concerns about the ability of the foreign entity to protect the Suspicious Activity Report. There are now over 107 foreign nations that have FIUs recognized by the Egmont Group which adhere to its Principles. Rather than imposing geographic limitations on access to SAR systems within an institution or its related entities due to disclosure fears, FinCEN should promote this established process to protect that information.

A second concern over foreign disclosure of sensitive data arises through private litigation in foreign civil courts. Just as in the United States, successful protection of SAR confidentiality is dependent on the assertion of their privileged status by the subpoenaed institution accompanied by supportive intervention by appropriate U. S. authorities. In the United States, that intervention is not accomplished by FinCEN acting independently but by the Justice Department acting at FinCEN's request or by the institution's primary federal regulator. A similar approach can apply to foreign civil process. Egmont Group FIUs share the concern for protecting SARs and the SAR process and would, like FinCEN, seek similar protection of SAR reports from civil process within their jurisdiction. In addition, foreign FIUs should be expected to enlist foreign supervisors to play a role similar to that exercised by U.S. regulators here to protect SAR reports from disclosure. Although litigation disclosure is never absolutely preventable, its risk is manageable by vigorous defense and easily implemented and coordinated strategies. Therefore, it does not make sense to use possible disclosure in a foreign private lawsuit as an excuse for geographic barriers to SAR sharing within an institution.

Comments on Other Aspects of the Proposed Guidance and Rules

Permissible Sharing by Securities Broker-Dealers, Mutual Funds, Futures Commission Merchants, and Introducing Brokers in Commodities with Certain U. S. Affiliates. Finally, a companion proposal would establish similar guidance for these securities companies to allow them to share SARs and SAR information. ABA and ABASA fully support having comparable guidance since it helps simplify and streamline compliance and also facilitates enterprise-wide risk management. We also support the provision in the proposed rule that reaffirms the ability to share SARs with law enforcement and supervisory agencies. Since self-regulatory organizations (SROs) serve a supervisory role similar to that held by financial regulatory agencies, allowing them access to SARs is also appropriate and should be comparable to the same access granted federal banking regulators. And, we recommend that the final rule clarify that the ability to share SARs with law enforcement includes federal and state regulators with enforcement authority over the financial institution.

Private Litigation. While ABA and ABASA support the provision that bars disclosure of SARs for use in private litigation, that provision raises two issues that also need to be addressed. The first is whether duplicate notification to both FinCEN and a bank's primary federal regulator is necessary. We believe it should be permissible for a bank to notify its primary regulator which in turn can and should notify FinCEN, since FinCEN has signed memoranda of understanding with the federal banking regulators and since FinCEN has delegated primary responsibility for supervision of BSA compliance to the banking agencies.

The second concern involves direct attack on the reporting process through private litigation. We fully support barring disclosure of SARs for use in private litigation and appreciate that the federal banking agencies have, over the years, been extremely helpful in preserving the integrity and confidentiality of SARs from litigation disclosure. However, there has been a recent trend of cases alleging that a bank did not take sufficient steps to address possible suspicious activities and that, as a result, the plaintiff suffered a loss. ABA and ABASA believe that, given the current state of the economy, this type of litigation is likely to continue. While we do not suggest that banks be allowed to raise a SAR as an affirmative defense, we would welcome the opportunity to work with FinCEN and the banking agencies to develop a solution to respond to these claims.

Finally, while the proposed rule would bar government agents from disclosing a SAR or information that would reveal the existence of a SAR in private litigation, we recommend the final rule clarify that this applies to both government agents *and* financial institutions. This would help underline the sanctity of SAR confidentiality. We believe that stressing confidentiality for *all* civil litigation will help avoid attempts by some attorneys to seek ways around the non-disclosure rule.

Conclusion

While ABA and ABASA firmly believe in the importance of protecting the confidentiality of SARs, we also strongly support permitting financial institutions to share SARs and SAR information across the enterprise-wide organizational structure. Unnecessarily limiting access to information not only impedes the ability of financial institutions to manage money laundering and related risks but also impairs their ability to detect and report suspicious activity. To ensure that financial institutions can develop the most effective systems, sharing of confidential SAR information across the enterprise as covered by a comprehensive AML/CFT compliance program is a necessary capability for many multi-national financial institutions. And, since previous guidance from the federal government acknowledges that financial institutions can share this data with their headquarters, no matter where that headquarters may be located, geographical restrictions on SAR sharing with affiliates or third-party service providers is illogical. Moreover, these restrictions undermine effective enterprise wide risk management (ERM) since free flow of information about SARs and SAR filing is integral to ERM. While there are risks associated with sharing information, appropriate controls can minimize risks, and an enterprise should be able to share information under the confines of its BSA compliance program.

Thank you for the opportunity to comment. ABA and ABASA look forward to continuing to work with FinCEN and the other federal regulators as well as law enforcement to streamline the rules to focus on the primary goal: detecting and deterring suspicious activities and doing it in a way that meets the goal of achieving true global cooperation for these initiatives.

If you have any questions or need additional information, please contact the undersigned by telephone at 202-663-5029 or by e-mail at rrowe@aba.com.

Sarah A. Miller
Executive Director & General Counsel
ABA Securities Association

Robert G. Rowe
Vice President & Senior Counsel
American Bankers Association

cc: Office of the Comptroller of the Currency
Office of Thrift Supervision