

One Small Step for AML: Federal Banking Regulators Issue Joint Statement on BSA/AML Resource Sharing

October 8, 2018 | Client Update | 5-minute read

The Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the federal banking regulators have taken a small step towards improving the BSA/AML compliance framework for depository institutions. These agencies issued a [Joint Statement on Banks and Credit Unions Sharing Resources to Improve Efficiency and Effectiveness of Bank Secrecy Act Compliance](#) (Joint Statement) on October 3, 2018 to address ways in which small banks and credit unions may enter into collaborative arrangements to share resources to manage their BSA/AML obligations. The Joint Statement was the result of a working group consisting of FinCEN, the federal banking regulators and the Treasury Department's Office of Terrorism and Financial Intelligence aimed at improving the effectiveness and efficiency of the BSA/AML regime.

Use of Collaborative Arrangements for BSA/AML Purposes

As described in the Joint Statement, "collaborative arrangements" involve two or more banks with the objective of (1) participating in a common activity or (2) pooling resources to achieve a common goal. Collaborative arrangements may be used by banks to pool human, technology, or other resources to reduce costs, increase operational efficiencies, and leverage specialized expertise. The Joint Statement specifically notes that collaborative arrangements for BSA/AML compliance management purposes are generally most suitable for banks "with a community focus, less complex operations, and lower risk-profiles for money laundering or terrorist financing".

The Joint Statement details a number of specific, non-exhaustive examples of situations in which the use of shared resources in a collaborative arrangement may be beneficial for banks in meeting their BSA/AML compliance program requirements, including:

- **Internal Controls:** sharing resources between two or more banks to conduct internal control functions, such as (1) reviewing, updating, and drafting BSA/AML policies and procedures; (2) reviewing and developing risk-based customer identification and account monitoring processes; and (3) tailoring monitoring systems and reports for the risks posed.
- **Independent Testing:** using personnel at one bank to conduct the BSA/AML independent test at another bank. Shared resources may be used in the scoping, planning, and performance of the BSA/AML compliance program independent test with appropriate safeguards in place to ensure the confidentiality of sensitive business information (and that the shared resource has the proper qualifications and is free of conflicts of interest arising from any involvement in the other bank's BSA/AML functions).
- **BSA/AML Training:** jointly hiring and sharing the costs of a qualified instructor to conduct required BSA/AML training. Examples of basic BSA/AML training topics that may be covered by shared resources include alert analysis and investigation techniques, alert trends and money laundering methods, and regulatory updates.

In contrast, the Joint Statement expressly notes that the sharing of a BSA officer among banks (other than affiliated banks) may not be appropriate for confidentiality and other reasons.

Impact on Sharing of Information

The Joint Statement specifically does not apply to – and therefore neither imposes a further limitation on, nor eases – arrangements or associations formed for the purposes of sharing information pursuant to Section 314(b) of the USA PATRIOT Act, a safe harbor provision that permits a broad range of financial institutions to share certain information related to potential money laundering or terrorist financing activities (but not Suspicious Activity Reports (SARs) or the fact that SARs have been filed). Collaborative arrangements described in the Joint Statement would not be associations for purposes of Section 314(b), which means that one or more financial institutions wishing to form an association for information sharing purposes would have to separately satisfy the applicable requirements under the USA PATRIOT Act and applicable FinCEN regulations.

Risk Management Implications of Collaborative Arrangements

The Joint Statement makes it clear that banks and credit unions, in implementing any BSA/AML collaborative arrangements, must effectively take into consideration existing supervisory guidance on outsourcing, vendor management and dual-hatted employees. In particular, the Joint Statement notes that:

- A bank's board of directors should provide appropriate oversight of collaborative arrangements in advance and, to the extent appropriate, should receive periodic reports about the arrangements;
- A bank's management should provide adequate oversight of the activities of shared resources, including through the receipt by senior management of periodic reports, and devote sufficient resources to monitoring services performed under the arrangements;
- Banks must comply with applicable legal restrictions relating to the disclosure of confidential supervisory information, confidential financial and business information, individual customer data, and trade secrets, and must also take into account potential antitrust issues and rules designed to limit conflicts of interest;
- Collaborative arrangements should be appropriately documented and should address the nature and type of resources to be shared, each institution's rights and responsibilities under the arrangement, procedures for protecting customer data and confidential information, and the management of risks associated with the sharing of resources; and
- Collaborative arrangements should be designed and implemented in accordance with the bank's risk profile for money laundering and terrorist financing.

Further Improvements Needed

While any improvement in the BSA/AML compliance framework is welcome, the Joint Statement is limited to addressing potential cost-saving and resource-sharing steps that smaller banks can take to reduce the burden of the existing BSA/AML requirements. It does not address the ability of banks of any size to cooperate in developing and accessing common information databases for purposes of customer due diligence and to facilitate analyzing transactions to determine whether they are suspicious. The existing restrictions on information sharing and access to information that other banks or law enforcement agencies may have about potentially suspicious transactions are among the most important factors contributing to the burden and inefficiencies experienced by banking organizations of all sizes under the current BSA/AML compliance framework, in addition to the process-focused supervisory approach to BSA/AML compliance and the absence of meaningful feedback on SARs filed by banks.¹ We hope that the Joint Statement represents the first step in a broader BSA/AML compliance review.

[**View as a PDF**](#)

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Luigi L. De Ghenghi

+1 212 450 4296
luigi.deghenghi@davispolk.com

John B. Reynolds III

+1 202 962 7143
john.reynolds@davispolk.com

Will Schisa

+1 202 962 7129
will.schisa@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.

¹ See, e.g., Greg Baer (President, The Clearing House Corporation), *Examining the BSA/AML Regulatory Compliance Regime*, Testimony before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit (June 28, 2017); The Clearing House, *A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement* (February 2017).