

Interagency Statement on Sharing Bank Secrecy Act Resources

October 3, 2018

Introduction

The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) (collectively, the Agencies), are publishing this statement to address instances in which banks¹ may decide to enter into collaborative arrangements to share resources to manage their Bank Secrecy Act (BSA) and anti-money laundering (AML) obligations more efficiently and effectively. Collaborative arrangements as described in this statement generally are most suitable for banks with a community focus, less complex operations, and lower-risk profiles for money laundering or terrorist financing. The risk profile is bank-specific, and should be based on a risk assessment that properly considers all risk areas, including products, services, customers, entities, and geographic locations.²

Collaborative arrangements involve two or more banks with the objective of participating in a common activity or pooling resources to achieve a common goal. Banks use collaborative arrangements to pool human, technology, or other resources to reduce costs, increase operational efficiencies, and leverage specialized expertise.

Notably, this interagency statement does not apply to collaborative arrangements or consortia formed for the purpose of sharing information under Section 314(b) of the USA PATRIOT Act. Further, banks that form collaborative arrangements as described in this interagency statement are not an association for purposes of Section 314(b) of the USA PATRIOT Act.³ Banks should contact FinCEN for additional information concerning the 314(b) program and requirements.

All banks are required to establish and maintain procedures reasonably designed to ensure compliance with the BSA and to develop and implement BSA/AML programs.⁴ The BSA/AML compliance program must include the following: 1) a system of internal controls to ensure ongoing compliance; 2) independent testing of BSA/AML compliance; 3) designating an individual or individuals responsible for managing BSA compliance (BSA compliance officer);

¹ Under the BSA the term "bank" is defined in 31 CFR 1010.100(d) and includes each agent, agency, branch or office within the United States of banks, savings associations, credit unions, and foreign banks.

² See Federal Financial Institutions Examination Council (FFIEC) *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (2014), at https://bsaaml.ffiec.gov/pages_manual/manual_online.htm

³ See *Voluntary Information Sharing Among Financial Institutions*, 31 CFR 1010.540.

⁴ See 31 U.S.C. 5311 *et seq.*, 31 U.S.C. 5318(h)(1), and the federal banking agencies' implementing BSA/AML compliance program regulations: 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (FRB); 12 CFR 326.8 (FDIC); 12 CFR 748.2 (NCUA); and 12 CFR 21.21 (OCC).

and 4) training for appropriate personnel.⁵ A bank is expected to have a BSA/AML compliance program commensurate with its respective risk profile.

Benefits of Sharing a Resource

The cost of meeting BSA requirements and effectively managing the risk that illicit finance poses to the broader U.S. financial system may be reduced through sharing employees or other resources in a collaborative arrangement with one or more other banks. These arrangements may also provide access to specialized expertise that may otherwise be challenging to acquire without the collaboration. The following examples describe situations in which the use of shared human, technology or other resources in a collaborative arrangement may be beneficial for banks. These examples are not intended to be exhaustive.

Internal Controls Example

Banks are required to provide for a system of internal controls to assure ongoing compliance with the BSA. A collaborative arrangement may be entered into by two or more banks to share resources between the respective banks to conduct internal control functions. Some examples of functions that may be conducted utilizing shared resources include: 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 Example

Banks are required to provide for independent testing for compliance. That testing may be conducted by an outside party or bank personnel. Such testing should provide an evaluation of the adequacy and effectiveness of the bank's BSA/AML compliance program.

Some banks may have personnel that perform multiple job functions, making it difficult to identify an employee within the bank to conduct an independent test of the BSA/AML compliance program. Personnel at one bank may be utilized to conduct the BSA/AML independent test at another bank within a collaborative arrangement. The shared resource may, for example, be utilized 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. The banks involved in the collaborative arrangement need to ensure that the shared resource conducting the BSA/AML independent testing is qualified and not involved in other BSA/AML functions at the bank being reviewed, such as training or developing policies and procedures that may present a conflict of interest or lack of independence.

⁵ See 31 CFR 1020.210 and 1010.230 – Under the Customer Due Diligence rule, banks are required to develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence, to include, but not be limited to (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information (including beneficial owners of legal entity customers).

BSA/AML Training Example

Banks must ensure that appropriate personnel are trained in BSA regulatory requirements and in internal BSA/AML policies, procedures, and processes.

It may be challenging to acquire personnel with BSA/AML expertise in some communities. It may also be cost prohibitive to attract a qualified outside BSA/AML trainer. A collaborative arrangement between two or more banks may provide the latitude to hire a qualified instructor to conduct the BSA/AML training, allowing the bank to share the cost. 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.

Other Considerations

The bank's board of directors must designate a qualified individual or individuals to serve as the BSA compliance officer.⁶ The sharing of a BSA officer among banks could be challenging due to the confidential nature of suspicious activity reports filed and the ability of the BSA officer to effectively coordinate and monitor each bank's day-to-day BSA/AML compliance. In addition, the sharing of a BSA officer may create challenges with effective communication between the BSA officer and each bank's board of directors and senior management. Accordingly, it may not be appropriate for banks to enter into a collaborative arrangement to share a BSA officer.⁷

Risk Considerations and Mitigation

The use of collaborative arrangements to manage BSA/AML obligations requires careful consideration regarding the type of collaboration in relation to the bank's risk profile, adequate documentation, consideration of legal restrictions, and the establishment of appropriate oversight mechanisms; and should be consistent with sound principles of corporate governance. For example, a bank's board of directors should provide for appropriate oversight of BSA/AML collaborative arrangements in advance. As is standard, a collaborative arrangement should be supported by a contractual agreement between the banks, with the performance reviewed by management and evaluated on a periodic basis. Banks should refer to their respective regulator's existing guidance regarding third-party relationships.

A collaborative arrangement for sharing employees or other resources to manage BSA/AML obligations is similar to using dual-employees. Guidance in this area could be relevant to contractual agreements between banks sharing BSA/AML resources.⁸ Banks must also comply with all applicable legal restrictions, including limitations on the disclosure of confidential supervisory information, confidential financial and business information, individual customer

⁶ See 12 CFR 208.63, 12 CFR 211.5(m), and 12 CFR 211.24(j) (FRB); 12 CFR 326.8 (FDIC); 12 CFR 748.2 (NCUA); and 12 CFR 21.21 (OCC).

⁷ Although it may not generally be appropriate to share a BSA officer through a collaborative arrangement, it may be more appropriate between affiliated banks.

⁸ See e.g., FDIC's *Risk Management Manual of Examination Policies*, Chapter 4.3 *Related Organizations, Dual Employees* Section at <https://www.fdic.gov/regulations/safety/manual/section4-3.pdf>.

data, and trade secrets, as well as restrictions governing collaborative arrangements among competitors generally, such as rules designed to limit conflicts of interest.

As is usual and customary when a bank enters into an arrangement with a third-party, a collaborative arrangement should be appropriately documented to define the nature and type of resources to be shared, define each institution's rights and responsibilities, establish procedures for protecting customer data and confidential information, and develop a framework to manage risks associated with the sharing of resources. Reasonable systems should be established to ensure that bank management adequately oversees the activities of shared resources. Banks should devote sufficient resources for monitoring services performed under the collaborative arrangement. Periodic reports related to BSA/AML collaborative arrangements should be provided to senior management and reported to the board of directors as appropriate in conjunction with their regular oversight of bank activities.

It is important that collaborative arrangements be designed and implemented in accordance with the bank's risk profile for money laundering and terrorist financing. Ultimately, each bank is responsible for ensuring compliance with BSA requirements. Sharing resources in no way relieves a bank of this responsibility. Nothing in this interagency statement alters a bank's existing legal and regulatory requirements.

Conclusion

Banks may benefit from using shared resources to manage certain BSA/AML obligations more efficiently and effectively. However, banks should approach the establishment of collaborative arrangements like other business decisions, with due diligence and thorough consideration of the risks and benefits. Banks are encouraged to contact their primary federal regulator regarding sharing BSA resources, and should refer to other relevant guidance.⁹

⁹ See e.g., OCC's "[An Opportunity for Community Banks: Working Together Collaboratively](https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-community-banks-working-collaborately.PDF)" (January 13, 2015), at <https://www.occ.gov/publications/publications-by-type/other-publications-reports/pub-other-community-banks-working-collaborately.PDF>.