

# Understanding BSA Violations<sup>1</sup>

The Bank Secrecy Act (BSA) and its implementing rules are not new; the BSA has been part of the bank examination process for more than three decades.<sup>2</sup> In recent years, a number of financial institutions have been assessed large civil money penalties for noncompliance with the BSA. While most insured financial institutions examined demonstrate an adequate system of BSA controls, these high profile cases highlight the importance of banks' efforts to ensure compliance with the BSA and its implementing rules. Nevertheless, where an institution falls short of these requirements, these shortfalls can result in violations of the BSA and the implementing rules being cited in Reports of Examination (ROE).

This article discusses the evolution of the BSA, including a brief overview of the USA PATRIOT Act (Patriot Act) changes. The article also discusses the types of BSA-related violations cited in examination reports, provides examples of best practices for maintaining a strong Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance program, and clarifies the distinctions between a significant BSA program breakdown and technical problems in financial institutions.

## Evolution of the BSA

The first Anti-Money Laundering (AML) statute, enacted in the U.S. in 1970, was titled *Currency and Foreign Transactions Reporting Act* and has become commonly known as the "Bank

Secrecy Act" or "BSA." The BSA established basic recordkeeping and reporting requirements for private individuals, banks and other financial institutions. The complexity of the BSA expanded in subsequent years with legislative changes requiring banks to establish procedures to ensure BSA compliance. Provisions were also added establishing criminal liability against persons or banks that knowingly assist in money laundering or structuring or that avoid BSA reporting requirements.

The most sweeping changes in the BSA occurred shortly after the September 11, 2001, terrorist attacks with the passage of the Patriot Act in October 2001.<sup>3</sup> The Patriot Act criminalized the financing of terrorism and augmented the BSA by strengthening customer identification procedures; prohibiting financial institutions from engaging in business with foreign shell banks; requiring financial institutions to have due diligence procedures, and, in some cases, enhanced due diligence procedures for foreign correspondent and private banking accounts; and improving information sharing between financial institutions and the U.S. government. The Patriot Act and its implementing regulations also

- Expanded the AML program requirements to all financial institutions;
- Increased the civil and criminal penalties for money laundering;
- Provided the Secretary of the Treasury with the authority to impose

<sup>1</sup> This article reflects the FDIC's practices to date and is not intended to be a legal interpretation. Information is provided to assist banks in complying with the law but is subject to adjustment as examination practices are reviewed or refined.

<sup>2</sup> By regulation, authority to examine for BSA compliance has been delegated to the regulator of each category of financial institution (i.e., the banking regulators for banks, the Securities and Exchange Commission for broker-dealers), and to the IRS for institutions that do not have a primary regulator. 31 CFR 103.56(b). The first rules delegating this authority were finalized in 1972. See 37 FR 6912, April 5, 1972.

<sup>3</sup> Refer to the *Supervisory Insights*, From the Examiner's Desk... Summer 2004 edition for a discussion of the USA PATRIOT Act and new regulations affecting the industry. See [www.fdic.gov/regulations/examinations/supervisory/insights/sisum04/sisum04.pdf](http://www.fdic.gov/regulations/examinations/supervisory/insights/sisum04/sisum04.pdf).

“special measures” on jurisdictions, institutions, or transactions that are of “primary money laundering concern”;

- Facilitated records access and required banks to respond to regulatory requests for information within 120 hours; and
- Required the Federal banking agencies to consider a bank’s AML record when reviewing bank mergers, acquisitions, and other applications for business combinations.

To ensure consistency in the BSA/AML examination process and provide guidance to the examination staff, the Federal banking agencies, the Financial Crimes Enforcement Network (FinCEN), and the Office of Foreign Assets Control released the *Federal Financial Institutions Examination Council’s Bank Secrecy Act/Anti-Money Laundering Examination Manual* in June 2005. The manual was updated and re-released in July 2006.<sup>4</sup>

---

## Required Elements of a BSA/AML Program

Federal law requires each financial institution to establish and maintain a BSA/AML compliance program. This program must provide for the following minimum requirements (also referred to as “pillars”) as outlined in Part 326.8 of FDIC Rules and Regulations:

- 1) A system of internal controls to ensure ongoing compliance.
- 2) Independent testing of BSA compliance.
- 3) A specifically designated person or persons responsible for managing BSA compliance (i.e., BSA compliance officer).
- 4) Training for appropriate personnel.

In addition, the Patriot Act required banks to establish a customer identification program, which must include risk-based procedures that enable the institution to form a reasonable belief that it knows the true identity of its customers. Referred to as the “fifth pillar,” this requirement was implemented in October 2003.

Examiners assess compliance in these areas during BSA/AML examinations. Relevant findings from transaction testing and recommendations to strengthen the bank’s BSA/AML compliance program, including its policies, procedures, and processes, are reflected within the ROE, and are an integral part of the FDIC’s risk management examination process. Examination findings may include violations of the BSA and the implementing rules. The next section takes a closer look at the different types of violations and discusses the significance of these types of violations in an overall BSA/AML program.

---

## BSA-Related Violations

For state-chartered, nonmember banks supervised by the FDIC, applicable BSA-related violations include infractions of FDIC Rules and Regulations (12 CFR 326.8 and 12 CFR 353), as well as, the Department of Treasury Regulations (31 CFR 103). These regulations, in addition to other applicable legal requirements, are summarized as

A body of statutes, regulations and administrative rulings, both Federal and State, is an element of the regulatory framework within which banks operate. Their underlying rationale is the protection of the general public (depositors, consumers, investors, creditors, etc.) by establishing boundaries and standards within which banking activities may be conducted.

---

<sup>4</sup> See FFIEC BSA/AML Examination Manual InfoBase, [www.ffiec.gov/bsa\\_aml\\_infobase/default.htm](http://www.ffiec.gov/bsa_aml_infobase/default.htm).

# Understanding BSA Violations

continued from pg. 23

The FDIC assigns a high priority to the detection and prompt correction of violations in its examination and supervisory programs.<sup>5</sup>

In general, there are three broad categories of violations that reflect noncompliance with BSA-related regulations:

- (I) Lack of an effective overall compliance program,<sup>6</sup> or specified components of a program (“pillar”);<sup>7</sup>
- (II) Systemic and recurring noncompliance with the BSA and implementing regulations; and
- (III) Isolated and technical noncompliance with the BSA.

Examiners document in the ROE instances of noncompliance with the BSA to develop and provide for the continued administration of a BSA/AML compliance program reasonably designed to assure and monitor compliance with the BSA. However, BSA compliance deficiencies range from isolated instances of noncompliance within an effective overall BSA/AML compliance program to serious weaknesses exposing the institution to an unacceptable level of risk for potential money laundering or other illicit financial activity. The distinction between these violations types is outlined below.

**(I) Program Violations.** Violations of the FDIC’s BSA/AML program rule are cited when *failure* occurs in the over-

all BSA/AML program. BSA program violations must be supported by at least one pillar violation. Violations of individual pillars might, or might not, lead to the conclusion that the bank has suffered an overall BSA/AML program violation. A BSA/AML program failure exposes the institution to an unnecessarily high level of potential risk to money laundering or other illicit financial transactions. The first possible indication that a BSA program has failed is by the absence of one or more of the required pillars. For example, a bank might have a lengthy period when there is no designated BSA compliance officer, or may have failed to provide necessary training.

A BSA/AML program *failure* can also be demonstrated by significant noncompliance, on a recurring or systemic basis, with the primary elements of the BSA related to recordkeeping and reporting of critical financial information,<sup>8</sup> as outlined in the Department of Treasury Regulations 31 CFR 103. Generally, examination reports citing BSA/AML program failures would include violations that demonstrate noncompliance with one or more of the primary elements of the minimum financial recordkeeping or reporting requirements. These requirements include

- Reporting suspicious transactions by filing Suspicious Activity Reports (SARs) [31 CFR 103.18];<sup>9</sup>

<sup>5</sup> From the FDIC’s *Risk Management Manual of Examination Policies* and applies to violations that may be cited for all types of examinations (e.g., Safety and Soundness, BSA, Information Technology).

<sup>6</sup> 12 CFR 326.8(b)(1) requires that each bank develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with recordkeeping and reporting requirements.

<sup>7</sup> 12 CFR 326.8(b)(2) and (c)(1) through (c)(4) require that a program specifically include: implementing a customer identification program; establishing system of internal controls; providing independent testing; designating a BSA Officer; and instituting a training program.

<sup>8</sup> The BSA, Titles I and II of Public Law 91-508, as amended, modified at 12 U.S.C. 1829b, 12 U.S.C. 1951-1959, and 31 U.S.C. 5311-5332, authorizes the Secretary of the Treasury, *inter alia*, to require financial institutions to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax, and regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, to protect against international terrorism, and to implement counter-money laundering programs and compliance procedures. Regulations implementing Title II of the Bank Secrecy Act appear at 31 CFR 103.

<sup>9</sup> Part 353 of the FDIC Rules and Regulations parallels 31 CFR 103.18, related to suspicious activity reporting requirements.

- Implementing a program to obtain and verify customer identification [31 CFR 103.121];
- Establishing procedures for responding to information requests made by law enforcement through the FinCEN, in accordance with the process provided for in Section 314(a) of the Patriot Act [31 CFR 103.100];
- Reporting large cash transactions through accurate and timely Currency Transaction Report filings (CTRs) [31 CFR 103.22]; and/or
- Documenting purchases and sales of monetary instruments and incoming/outgoing wire transfers [31 CFR 103.29 and 31 CFR 103.33].

To affect corrective action when a BSA/AML program violation is cited, the FDIC will issue a cease and desist order as required under Section 8(s) of the *Federal Deposit Insurance Act*.

### **(II) Systemic and Recurring**

**Violations.** Regardless of whether a program failure which falls under Section 8(s) is found, an examiner could find systemic violations which relate to ineffective systems or controls to maintain necessary documentation or reporting of customers, accounts, or transactions, as required under various provisions of 31 CFR 103. Determining whether such violations are systemic may be influenced by the number of customers, accounts, or transactions affected; the importance of the unavailable or unrecorded information; the pervasive nature of noncompliance; the predominance of violations throughout the organization; and/or certain program elements that do not adequately provide for an effective system of reporting. Examples of violations that may result in systemic violations include

- Habitually late CTR filings across the organization;
- A significant number of CTRs or SARs with errors or omissions of critical data elements;

- Consistently failing to obtain critical customer identification information at account opening; and
- Systems and programs that do not allow for proper aggregation of multiple cash transactions for regulatory reporting purposes.

Systemic violations of the BSA represent significant noncompliance with financial recordkeeping and reporting requirements or reflect failures within one or more pillars of a BSA/AML program, if not the overall BSA/AML program.

### **(III) Isolated and Technical**

**Violations.** Isolated and technical violations are those limited instances of noncompliance with the financial recordkeeping or reporting requirements of the BSA that occur within an otherwise adequate system of policies, procedures, and processes. Despite the adequacy of the overall program, examiners may note minor violations regarding limited, isolated individual transactions and will focus ROE comments on critical missing or incorrectly reported information for those transactions. These types of violations do not generally result in significant concerns over management's administration of the overall BSA/AML program. Further, when such violations are correctable and management is willing and able to implement appropriate corrective steps, a formal supervisory response may not be warranted.

---

## **The Best Defense Is a Good Offense**

The steps a bank should take to ensure compliance with the BSA and its implementing rules are documented extensively and are consistent with guidelines that existed before the implementation of the Patriot Act: *To avoid the most serious violations and the implications that can result when those violations are cited, banks must have a strong BSA/AML compliance program.*

# Understanding BSA Violations

continued from pg. 25

Financial institutions should ensure they have a well-developed and documented risk assessment that accurately captures the risk exposures of their products, services, customers, and geographic locations. Exposures identified through the risk assessment should be addressed in policies and procedures making sure all identified risks are addressed. Monitoring programs should be in place to ensure account and transaction activity is consistent with expectations and to identify and report suspicious activity. A strong training program should ensure that appropriate personnel are familiar with regulatory requirements and bank policies. The compliance program should be subjected to a periodic independent test of BSA/AML controls to verify compliance with the financial institution's BSA/AML program. The test plan and its results should be reviewed by management to ensure corrective action is taken and the scope of testing meets the bank's requirements. Finally, the bank should have a qualified employee designated by

the board of directors to oversee BSA functions and ensure that regulatory requirements and bank policies are being followed on a day-to-day basis.

While banks have long been required to have an appropriate BSA program, including policies, procedures, and processes in place to ensure BSA compliance, passage of the Patriot Act has resulted in a number of sweeping changes to the BSA. Understanding the main components of a strong BSA compliance program will help banks to appropriately implement these changes and future amendments.

For additional information on BSA/AML, refer to the Federal Financial Institutions Examination Council's (FFIEC's) BSA/AML InfoBase. (See [http://www.ffiec.gov/bsa\\_aml\\_infobase/default.htm](http://www.ffiec.gov/bsa_aml_infobase/default.htm).) The InfoBase is intended to be a one-stop resource for BSA compliance. In addition to the FFIEC BSA/AML Examination Manual, the InfoBase includes, for example, a list of frequently asked questions, various forms needed for meeting BSA/AML compliance responsibilities, and links to the various BSA/AML laws and regulations.

Table

Best Practices for BSA/AML Compliance
1) Comprehensive Risk Assessment
2) Appropriate Policies and Procedures
3) Adequate Monitoring Programs
4) Strong Training Programs
5) Thorough Independent Testing
6) Qualified Employee Overseeing Day-to-Day Operations

**Debra L. Novak**  
*Chief, Anti-Money Laundering Section*  
*Washington, D.C.*

**Charles W. Collier**  
*Senior Program Analyst,*  
*Anti-Money Laundering Section*  
*Washington, D.C.*