Lawdesk

Bank Secrecy Act

Once upon a time, a seemingly long time ago, *Bank Secrecy Act* ("BSA") compliance was a routine exercise that revolved around the proper completion and submission of government forms. During the past few years; however, BSA compliance has taken on a life of its own and is now anything but routine. In the words of Dan Stipano, Deputy Chief Counsel for the Office of the Comptroller of the Currency, taking a "business as usual approach" with respect to the BSA is no longer sufficient.

Bank Secrecy Act (BSA)

Bank Secrecy Act ("BSA") / Anti-Money Laundering ("AML"):

- The focus of the BSA is to prevent banks and other financial institutions from being used as intermediaries for criminal activity and to help law enforcement agencies investigate money-laundering schemes.

The Bank Secrecy Act requires all financial institutions to:

- Monitor suspicious customer behavior.
- File reports on transactions that meet certain dollar amounts.
- Maintain records of suspicious activity.
  - ✓ The Suspicious Activity Report ("SAR") documents any known or suspected federal violation of federal law.

Company BSA Policy:

- Is to be familiar with the BSA requirements, implement appropriate policies and procedures to remain in compliance, train staff to be aware of compliance responsibilities and file reports in a timely manner.

The Board of Directors:

- Has appointed a BSA Officer to perform day-to-day monitoring of various functions within designated areas of BSA responsibility.
- The Board reviews the BSA Policy annually.

Bank Secrecy Act (BSA)

A Suspicious Activity Report must be filed on any known or suspected federal violation of law. Suspicious activity requires reporting if you know or suspect that, for example:

- The funds are derived from illegal activities.
- The funds are part of a plan to violate or evade any federal law or regulation.
- The transaction is designed to evade other reporting requirements.
- The transaction is not the sort in which the particular customer would normally be expected to engage, and the Company knows of no reasonable explanation for the transaction.

The Act requires reporting of any known or suspected violation if:

- An insider is involved, regardless of amount.
- The aggregate amount involved is $5,000 or more and a suspect can be identified.
- The aggregate amount involved is $25,000 or more and the suspect cannot be identified.
- Transactions aggregating $5,000 or more involved potential money-laundering or violation of the BSA.

Other types of reportable activities and examples:

- Computer Intrusion
- Counterfeit Credit/Debit Card
- Credit/Debit Card Fraud
- Misuse of Position
- Identity Theft

Bank Secrecy Act (BSA)

USA PATRIOT Act:

- As a result of 9/11/01, the BSA was amended to provide Federal government agencies with more authority to better identify, deter and punish international money laundering.
- The Act governs minimum standards for identification and verification of customers opening new accounts. It requires the Company to verify the identity of any person opening a new account, to the extent reasonable and practicable, and to maintain records of the information used to verify a person's identity. The Customer Identification Program ("CIP") was created in compliance with these requirements.
- Section 314(a) of the Act requires sharing information between law enforcement and financial institutions regarding suspected terrorist acts or money laundering activities. The Company monitors for this activity and reports true-named matches as applicable.

Office of Foreign Assets Control ("OFAC"):

- OFAC is part of the U.S. Treasury Department and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists and international narcotics traffickers.
- OFAC laws requires the Company to identify any transactions and property subject to the economic sanctions.
- While true name matches are not common, they are possible.
- The Company monitors new false-positive matches per month.

Bank Secrecy Act (BSA)

The Company encourages a BSA/AML compliance culture by ensuring that…

- ✓ Its management and staff understand the purpose of its BSA/AML efforts and how its reporting is used.
- ✓ Efforts to manage and mitigate BSA/AML deficiencies and risks are not compromised by revenue interests;
- ✓ Relevant information from the various departments within the organization is shared with Compliance staff to further BSA/AML efforts;
- ✓ It devotes adequate resources to its compliance function; and
- ✓ The Compliance Program is effective by, among other things, ensuring that it is tested by an independent and competent party.

Bank Secrecy Act (BSA)

Penalties for Noncompliance

Violations of BSA requirements may hold civil and/or criminal penalties, such as:

- Civil penalties of **$1,000** per day for each day of noncompliance.
- A penalty of **$500** per violation of the recordkeeping requirements of the BSA.
- Willful violations may cause civil penalties in an amount equivalent to that of the transaction (up to **$100,000**) or **$25,000**, whichever is greater.
- Continued noncompliance can result in the issuance of a "Cease & Desist" order from the FDIC.

Employees who fail to comply with the requirements of the BSA are subject to counseling and/or termination of employment.

Bank Secrecy Act (BSA)

Questions & Answers