

must adjust the value of the asset on its books, since it has not received the securities. The asset must be marked to the market and a 15% haircut taken on that current market value.

ANTI-MONEY LAUNDERING (AML) COMPLIANCE PROGRAM

Money laundering in its original sense is the concealment of the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses. Criminals might acquire “dirty” money through such activities as extortion, insider trading, drug trafficking, illegal gambling, and tax evasion. If the “dirty” money can be “laundered” by sending it abroad or using it to finance local businesses, comingling it with “clean” money, the authorities would have a hard time linking it to crime.

There are three stages of money laundering as traditionally defined:

1. **Placement** is the state of moving criminal (“dirty”) money into the financial system.
2. **Layering** is the shifting of funds among various accounts to confuse the origin of the assets.
3. **Integration** is the movement of the layered funds back into authentic investments (yielding “clean” money).

Since September 11, 2001, the definition of money laundering has been broadened to focus on using “clean” money for “dirty” purposes, such as funding terrorism.

The **Bank Secrecy Act of 1970** (BSA; also known as the Currency and Foreign Transactions Reporting Act) requires financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering. The BSA is sometimes referred to as an anti-money laundering (AML) law, or more specifically as BSA/AML. The USA PATRIOT Act broadened the scope of the BSA to focus on terrorist financing as well as money laundering.

The documents filed by businesses under the BSA requirements are used by domestic and international law enforcement agencies to identify, detect, and deter money laundering, which might be used to further a criminal enterprise, terrorism, tax evasion, or other unlawful activity. The Bank Secrecy Act established the U.S. Treasury Department as the lead agency for developing regulations related to anti-money laundering programs. The legislation is enforced by the **Financial Crimes Enforcement Network (FinCEN)**, a bureau within the Treasury Department.

The **Office of Foreign Assets Control**, also a part of Treasury, administers sanctions against trading with enemies of the U.S. These enemies listed by OFAC could be individuals, such as terrorists, narcotics traffickers, or money launderers, or they could be foreign governments. Financial institutions are required to block financial transactions by these sanctioned persons and countries and to either block or reject transactions with anyone trying to do business with them. To comply with this requirement, financial institutions must establish surveillance programs to check all international transactions against the

OFAC lists. Financial institutions must report to OFAC all blockings and rejections of sanctioned activities within *ten days* of identifying them.

FINRA requires each member to develop and implement a written anti-money laundering program designed to achieve and monitor the member's compliance with the requirements of the Bank Secrecy Act. The program must designate an individual to be the AML officer who is in charge of the program. The program must provide ongoing training to its employees and be reviewed annually.

In addition, member firms are required to establish in writing and implement policies, procedures, and internal controls designed to achieve compliance with the reporting and recordkeeping requirements of the Bank Secrecy Act. Financial institutions must keep or report the following:

- **Monetary Instrument Log (MIL)**—a record of cash purchases of negotiable instruments between \$3,000 and \$10,000. This record must be maintained for a minimum of five years.
- **Currency Transaction Report (CTR)**—a report sent to FinCEN of cash transactions that exceed \$10,000 in a single day, whether conducted in one transaction or several smaller ones.
- **Suspicious Activity Report (SAR)**—a report to the U.S. Treasury on any client who appears to be avoiding Bank Secrecy Act reporting requirements or is behaving in a way that suggests money laundering or some other illegal activity. See the next section for details.

Each member's anti-money laundering program must be approved, in writing, by a member of senior management. The Bank Secrecy Act mandates that all reports and documentation related to MILs, CTRs, and SARs be kept on file for five years from the date of the filing.

CURRENCY TRANSACTION REPORTS (CTRs)

The Bank Secrecy Act requires broker-dealers to report any currency received in the amount of more than \$10,000 in a 24-hour period, whether in one transaction or two or more smaller ones, by or on behalf of one person. The report is made to FinCEN using its CTR. The report must be filed within 15 calendar days of the transaction(s).

To comply with this law, financial institutions must obtain personal identification information about the individual conducting the transaction such as a Social Security number and driver's license or other government-issued document. This requirement applies whether the individual conducting the transaction has an account relationship with the institution or not.

SUSPICIOUS ACTIVITY REPORTS (SARs)

A Suspicious Activity Report is a report to the U.S. Treasury on any client who appears to be avoiding Bank Secrecy Act reporting requirements or is behaving in a way that suggests money laundering or some other illegal activity is occurring. Member firms and their employees are prohibited from disclosing to anyone believed to be involved in the suspicious activity that it has been reported. If the firm receives a subpoena for the information, it must refuse to provide the information unless disclosure is required by FinCEN, the SEC, an SRO such as FINRA, or another law enforcement authority.

A Suspicious Activity Report must be filled out whenever a client makes a transaction in excess of \$5,000 and the broker-dealer knows or suspects foul play, specifically if the transaction seems to have:

- Arisen from illegal activity or attempted to disguise funds or assets derived from illegal activity
- Attempted to avoid reporting requirements or other laws or regulations
- Served no apparent business or lawful purpose

The USA PATRIOT Act requires firms to make and retain records relating to wire transfers of \$3,000 or more. Required information includes the name and address of both sender and recipient, the amount of the transfer, the name of the recipient's financial institution, and the recipient's account number.

SARs must be filed with FinCEN no later than 30 days after the date the suspicious activity was detected. Copies of each SAR filing and related documentation must be kept for five years from the date of the filing.