The Complete Compliance and Ethics Manual

Anti-Money Laundering Compliance Programs for Financial Institutions and Other Businesses

By Stephanie Brooker and Linda Noonan

Introduction

- A doctor in Montana who dispenses a bogus cancer medication hires a lawyer to set up a trust in a Caribbean jurisdiction to hide his profits from patients suing him for malpractice. Funds are sent through the doctor’s brokerage account, which has little investment activity.

- A manufacturer of farm equipment in Kansas sells tractors to a Colombian distributor and is paid by a third party with a wire transfer from an account at a bank in Atlanta.

- A mid-level drug dealer in Los Angeles arranges with his friend who owns a record company to buy the cash that the drug dealer receives from street sales in exchange for checks drawn on the record company’s commercial bank account.

- A high-end jewelry store in Chicago sells a large engagement ring to a foreign government official and receives payment by wire from an offshore company the customer says he owns. The customer later says his fiancée has changed her mind and returns the ring. Instead of a refund, he asks the store to maintain a credit balance for future purchases.

- A Swiss company wires hundreds of thousands of dollars to the checking
account of an exchange student at a small community bank in Massachusetts in the town where she attends college. The student, who is the daughter of a notorious African dictator, then writes checks on the account to purchase several luxury vehicles and arranges for them to be shipped to her home country.

- An immigrant family routinely skims cash from their successful US business and uses the funds to purchase cashier’s checks at various banks in the United States and Canada. Family members deposit the cashier’s checks to an account for a charity controlled by a terrorist organization in a Middle Eastern country.

- A network of Chinese immigrant smugglers extorts money from recently arrived immigrants in Seattle and wires the funds through a dishonest agent of a reputable money transmitter to an import-export company in China. The dishonest agent structures the funds he receives into smaller transactions to avoid detection by the money transmitter and by law enforcement.

- A casino receives payment on casino debt from a patron who owns a chain of hardware stores across the United States. Payment comes from multiple offshore accounts, including accounts at nonbank financial institutions.

- A Chinese “manufacturing” customer of a Chinese bank with a correspondent account at a New York bank sends wire transfers routinely through this correspondent account to Mexican businesses.

- A Russian couple purchases a multimillion-dollar mansion in Silicon Valley in an “all cash” (no financing) transaction, with a check drawn on an account in the name of a trust registered in Guernsey.

What do all these people and the businesses and financial institutions with which they do business have in common? They are all involved in one way or another with some form of money laundering.

**What is Money Laundering?**

Money laundering is the process by which the existence, nature, or source of the proceeds of criminal activity is concealed or disguised to make the proceeds appear legitimate. Although money laundering is frequently associated with
drug trafficking, money laundering sustains all types of criminal activity that generate proceeds—drug trafficking, public corruption, fraud, alien smuggling, and traditional organized crime activities. Money laundering often figures in fiscal law violations—tax evasion, violations of currency controls, and customs violations. Money laundering also supports terrorism. Criminals must launder their ill-gotten gains to sustain and grow their enterprises and to enjoy the fruits of their labor without detection by government authorities.

Experts disagree on how to measure the money laundering problem or whether its extent can even be measured accurately. All agree that money laundering is a problem of staggering proportions and that, despite the best efforts of governments around the world for the last 30 years, the overall level of money laundering does not appear to be decreasing.

How is Money Laundered?

Money laundering schemes can be very simple or extremely complex depending on the imagination and needs of criminals and their lawyers and financial advisers. While not all money laundering schemes fit the model, it has become commonplace to speak of money laundering as having three stages, based on an analytical model developed by the Central Intelligence Agency in the late 1980s. The three stages are called placement, layering, and integration.

**Placement** – The physical disposal of bulk cash or its initial placement in the financial system, e.g., by using the cash proceeds from street sales of drugs to buy money orders or traveler’s checks or by depositing the cash into bank accounts in amounts of $10,000 or less to avoid cash reporting requirements.

**Layering** – The creation of layers of financial transactions to distance the funds from their illegal source, e.g., by purchasing goods with multiple money orders or by depositing the money orders into an account at one bank and wiring the funds to an account at a second bank.

**Integration** – Reaching the stage of apparent legitimacy for the funds, e.g., using bank deposits to purchase luxury goods, a business, or real estate.

The term “money laundering” conjures images from films of the mafia counting piles of cash in back rooms. Money laundering from drug trafficking as well as from many forms of traditional organized crime often does start with cash. Contrary to common belief, however, money laundering does not always
involve cash. For instance, money laundering related to various forms of fraud, high-level public corruption by the so-called kleptocracy regimes, or trade-based laundering, e.g., where illegitimate funds can flow across borders masked by the undervaluing or overvaluing of imports or exports, and may involve checks, wire transfers, loans, and/or letters of credit.

**The Government Response**

In the United States and in most other countries, governments have taken on the fight against money laundering by criminalizing money laundering activity, making the proceeds subject to forfeiture, and imposing regulatory requirements on financial institutions and other businesses to prevent and detect money laundering. Financial institutions and other businesses have implemented anti-money laundering (AML) programs in response to these government measures to fulfill their legal and ethical responsibilities not to facilitate money laundering, terrorism, or other crimes, and to protect against the reputational risk of being named in an indictment, forfeiture action, or negative press.

**The Crime of Money Laundering and the Related Forfeiture Authority.**

Since 1986, it has been a crime under US law to engage in virtually any financial transaction with the proceeds of “specified unlawful activity” with “knowledge” that the funds involved are the proceeds of some form of illegal activity. Specified unlawful activities (SUAs) include hundreds of crimes, from drug trafficking and securities fraud, to foreign and domestic public corruption. A person can be liable for money laundering without knowing which specific crime generated the proceeds, so long as the prosecution can prove that the funds in fact were the proceeds of any of the SUAs and that the person knew that the proceeds were derived from a violation of federal, state, or foreign law. Knowledge also can be based on willful blindness or deliberate indifference to the source of the funds; i.e., failure to make inquiries in the face of red flags of suspicious activity. In addition, money laundering can be based on a government sting where the funds are represented by the undercover agent to be the proceeds of illegal activity. The penalties for money laundering are severe—up to 20 years imprisonment and large fines for each violation.

Not only can the funds of the person convicted of money laundering be forfeited, but there can be civil forfeiture of any funds or other property.
involved in, or traceable to, the money laundering activity, even if no one has been prosecuted and even if the funds are no longer in the hands of the wrongdoer. If a civil forfeiture action is brought against property involved in or traced to money laundering, the person only may defeat the forfeiture by establishing that the person was an “innocent owner”—took the property without knowledge of the illegal activity.

Why the Need for AML Programs?

How can a financial institution or other business protect itself and its employees against money laundering liability and forfeiture actions if it becomes involved, even inadvertently, in money laundering? The best defense is a good offense—by establishing a fully-implemented AML program. AML programs are required for some financial institutions or financial businesses pursuant to specific regulatory requirements, discussed below, and are necessary for other businesses to help avoid potential criminal liability and forfeiture actions, as well as to protect the integrity of the organization and its directors, officers, and employees. The contents of an AML program can vary widely depending on the nature of the business; the money laundering risks to which the business is exposed with respect to its customers, its products and services, its geographic locations and markets; and the specific AML regulatory requirements and regulatory expectations applicable to the business.

Companies can obtain insight into the government’s expectations for AML programs from the Department of Justice’s Principles of Federal Prosecution of Business Organizations, which sets forth what a prosecutor must consider in deciding whether to charge a corporation with a crime. Prosecutors are directed to consider whether there is a compliance program that is “adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives.” To make this determination, prosecutors are to consider not only whether there is a compliance program on paper, but also if the program was designed, implemented, reviewed, and revised in an effective manner, including by determining whether there was sufficient staff to audit the program and whether adequate information about the program was disseminated to staff.

The potential punishment that could be imposed also will figure in determining
whether to charge a business itself (as opposed to specific employees of the business) with a crime. In that regard, further guidance on what should be included in an AML program can be found in the Federal Sentencing Guidelines Manual for business organizations. The Federal Sentencing Guidelines Manual sets out the elements of effective compliance and ethics programs to prevent and detect criminal conduct. Compliance and ethics programs should be “reasonably designed, implemented, and enforced so that the program is generally effective in preventing and detecting criminal conduct” and should include knowledge about the program by the organization’s “governing authority,” employee background screening, periodic evaluation of the effectiveness of the program, a mechanism to report criminal conduct internally, including anonymously, and reasonable steps to ensure compliance with the program.

While not directly related to money laundering prosecutions, it also is useful to review the publication of the Fraud Section of the Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs, which further expands on what DOJ will look for in a compliance program if a violation occurs.

In 2014, the Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) issued an Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance. This document also offers insight into government expectations for AML programs. The tenets of the document apply equally to any business’s AML program, not just those of financial institutions:

1. Leadership, management, and the board must be visibly and actively engaged in creating a culture of compliance;

2. Compliance should not be compromised by revenue interests;

3. Information should be shared within different areas of the organization to facilitate identifying potential suspicious activity; and

4. The AML compliance function must have adequate authority and independence and be supported by adequate staffing and technology resources.

The existence of a strong compliance and ethics program that meets these standards is not an ironclad guarantee, but it should go a long way in
protecting a financial institution or other business against criminal liability, and should help to establish an innocent ownership defense in the event of a forfeiture action.

**AML Programs for Financial Institutions – The Bank Secrecy Act**

**Overview**

The contents of the AML programs of financial institutions are driven not only by the need to protect against potential criminal liability, but also by specific regulatory requirements, regulatory guidance, and ever-increasing regulatory expectations. The main legal authority for AML requirements applicable to financial institutions—reporting, recordkeeping, and AML program requirements—is the Bank Secrecy Act, as amended by the USA PATRIOT Act, and its implementing regulations, (collectively, the BSA).\[10\] As used in this article, “Financial institution” applies broadly to all financial institutions and financial businesses subject to requirements under the BSA. Only certain of these meet the BSA regulatory definition of financial institution.\[11\] The AML program requirements apply to all the businesses subject to BSA requirements, but certain others only apply to those that come within the BSA regulatory definition of “financial institution.”

The BSA statute was enacted in 1970, long before money laundering was a criminal offense and, for many years, was the main weapon used to prosecute money laundering. The BSA provides the secretary of the Treasury with the authority to require financial institutions to file reports and maintain records; to take other AML measures useful for criminal, tax, and regulatory investigations and proceedings; and to combat terrorism. The BSA statutory requirements generally are not self-executing and must be implemented by regulation. In some cases, financial institutions also are subject to parallel requirements of their primary federal regulator or their self-regulatory organization (SRO), such as the Financial Industry Regulatory Authority (FINRA).

What constitutes a “financial institution” under the BSA is broadly defined in 31 U.S.C. § 5312(a)(2). To date, AML program requirements have been imposed
by BSA regulation on:

- banks (including thrifts and credit unions),
- broker-dealers in securities,
- futures commission merchants and introducing brokers in commodities,
- mutual funds,
- insurance companies, [12]
- money services businesses (MSBs), [13]
- casinos and card clubs,
- dealers in precious metals, jewels, and stones,
- operators of credit card systems (like Visa, MasterCard, Discover, and American Express),
- non-bank residential mortgage lenders and originators,
- housing government-sponsored enterprises (Fannie Mae and Freddie Mac).

Regulations to impose AML program and suspicious activity reporting on registered investment advisers have also been proposed.[14]

There are a number of other businesses listed in the BSA statute that potentially could become subject to BSA requirements by regulation, e.g., other types of loan and finance companies, travel agents, pawnbrokers, vehicle sellers, and persons involved in real estate settlements and closings; however, regulation of these businesses does not appear imminent. As of September 2019, under BSA geographic targeting orders, title insurance companies are subject to temporary BSA requirements in certain metropolitan areas relating to cash (non-financed) high-end residential real estate purchases by shell companies.[15] These areas include all boroughs of New York City; Miami-Dade, Broward, and Palm Beach Counties in Florida; Los Angeles County; San Francisco, San Mateo, and Santa Clara Counties; San Diego County; Bexar County; Texas (San Antonio); Honolulu County in Hawaii; Clark County in
Nevada (Las Vegas); Suffolk and Middlesex Counties in Massachusetts (Boston); Cook County in Illinois (Chicago); and King County in Washington (Seattle).

The BSA requirements for financial institutions do not apply extraterritorially, but only to financial institutions located in the United States, including offices, branches, and subsidiaries of foreign-owned institutions. MSBs that conduct business “wholly or in substantial part” in the United States, i.e., have a substantial percentage of their transaction activity with U.S. customers, however, are subject to the BSA requirements for MSBs even if they have no physical presence in the United States.

The BSA is administered and enforced by FinCEN, and, through delegations, the responsibility for examining financial institutions for compliance with the BSA has been given to the federal functional regulators and the SROs with respect to the financial institutions for which they are responsible. If a category of financial institution has no federal functional regulator—e.g., MSBs, casinos and card clubs, nonbank residential mortgage lenders and originators, and insurance companies—the delegation is to the Internal Revenue Service (IRS). FinCEN has no examination staff, although compliance and enforcement personnel do participate in selected exams.

There are stringent criminal and civil penalties for BSA violations in addition to the criminal penalties discussed above relating to 18 U.S.C. §§ 1956–1957. Penalties can be imposed not only on the financial institution or business, but also on its officers, directors, or employees. Both civil and criminal penalties can be imposed for the same violations under the BSA. BSA violations also are subject to the full range of enforcement authorities of the regulators. In addition to large civil monetary penalties by FinCEN and/or the regulators, civil or regulatory enforcement can include requiring financial institutions to undertake expensive remedial steps or undertakings, including detailed and frequent reporting, hiring independent consultants, look backs to identify previously unreported suspicious activity, and/or upgrades of customer due diligence. In cases where there have been serious breakdowns in BSA internal controls, resulting in a financial institution becoming involved in criminal activity, there have been a number of coordinated or parallel civil and criminal settlements, including prosecutions or deferred prosecutions and forfeitures based on the BSA criminal violations.

We have identified 30 criminal dispositions to-date involving financial
institutions based on BSA violations.

The BSA/AML Program Requirements

The specific BSA reporting and recordkeeping requirements vary for the different categories of financial institutions.[16] All financial institutions under the BSA regulations are required to develop, implement, and maintain written AML programs reasonably designed to prevent money laundering and terrorist financing. There are four required core elements of an AML program for financial institutions under the BSA. AML programs must:

- Incorporate policies, procedures, and internal controls to comply with the program and the specific BSA requirements applicable to the financial institution;
- Designate a compliance officer or officers with day-to-day responsibility for compliance with the program;
- Provide education and training of appropriate personnel about their responsibilities under the program; and
- Provide for periodic independent testing of the program.

For some financial institutions, a Customer Identification Program, and, effective in May 2018, a Customer Due Diligence Program, must be elements of their AML program, as discussed below.

1. Risk-Based AML Programs.

FinCEN and the financial institution regulators expect financial institutions to implement risk-based AML programs based on a formal risk assessment that must be refined on an ongoing basis. The risk assessment should take into consideration the institution’s products, services, and transactions; the nature of its customers; the geographic locations of the financial institution and the geographic characteristics of its customers, e.g., whether customers include citizens of, persons organized in, or persons doing business in jurisdictions that pose a high risk for money laundering, public corruption, or terrorism; and the strength of the financial institution’s BSA/AML controls to address the risks. Regulators are expecting more and more sophisticated risk assessments with quantitative and qualitative analysis to assess the inherent risk of the
institution and the residual risk once compliance controls are applied to the inherent risk.

If a financial institution is part of a financial group, and especially if it is part of a large or complex financial institution organization, FinCEN and the banking regulators encourage risk assessment and risk management at the enterprise level, e.g., by the holding company or lead financial institution, and they consider it a sound practice for a complex financial institution organization to implement an enterprise-wide AML program that manages risks in an integrated fashion across affiliates, business lines, legal entities, and risk types.\[17\]

Once developed, the risk assessment should drive the functioning of the AML program—for instance, what compliance and audit resources are needed and where to concentrate them, what systems are required to support the program, how transactions are monitored to identify suspicious activity and at what thresholds, and what level of due diligence is conducted on higher-risk customers and how often that information must be updated.

2. Formalizing and Documenting the AML Policy and Program and Program Governance.

The BSA regulations or parallel regulatory requirements specify who must approve the program, e.g., for banks, it is the board of directors.\[18\] Generally, there should be a BSA/AML policy and program document outlining the institution’s policy and program and applicable legal and regulatory requirements, and more detailed policies, procedures, and documented internal controls governing each element of the program and each BSA requirement. It is advisable that the policy clearly state the commitment of the board and senior management to BSA/AML compliance and to taking reasonable measures to prevent and detect money laundering, as well as when and how the program will be evaluated and revised to maintain its effectiveness. The responsibilities and expectations for everyone with a role in BSA/AML compliance—the board, senior management, business line management, the BSA officer and compliance staff, the legal department, security department, operations staff, internal audit, human resources, and employees generally—should be articulated clearly. The policy may set forth what types of clients the financial institution will not do business with because of legal prohibitions or restrictions (e.g., persons subject to sanctions...
administered by the Department of Treasury’s Office of Foreign Assets Control (OFAC) internet gaming businesses and their principals, marijuana businesses and their principles, and foreign shell banks; or because the burden of managing effectively the high compliance or reputational risk posed by a category of customer is deemed too great). The policy also should state the consequences of failure to comply with the BSA or the financial institution’s related policies and procedures. There should be routine governance reporting on the implementation of the program or any significant issues to senior management and the board.

While each financial institution under the BSA must have a separate AML program, holding companies or lead financial institutions of financial groups also should consider establishing an enterprise-wide AML policy and program that is approved by their board of directors.

3. Written Policies and Procedures and Documented Internal Controls.

All policies, procedures, and internal controls should be well-documented and up-to-date, and reasonably designed to ensure compliance with all applicable BSA requirements and the financial institution’s AML program. Careful consideration should be given to the timing of rolling out new policies, procedures, and systems to ensure that they have been tested and that adequate staffing is in place to implement them. As noted, the BSA recordkeeping and reporting requirements vary considerably depending on the type of financial institution, with the fullest range of requirements applicable to banks, broker-dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities. Some of the key requirements are summarized below:

a. Currency Reporting for Financial Institutions and Cash Reporting for Other Businesses. Because cash figures prominently in many money laundering schemes and in tax evasion, a concern for all US businesses—financial institutions and nonfinancial institutions—is compliance with cash reporting requirements. There is one cash reporting regime for businesses defined as financial institutions under the BSA, and another for other BSA financial businesses subject to BSA regulations and all other US trades or businesses under parallel BSA and IRS regulations.

Under 31 C.F.R. § 1010.310, financial institutions[19] must electronically file Currency Transaction Reports (CTRs) on all transactions in currency over
$10,000 conducted by or on behalf of the same person on the same business day. Transactions in currency include deposits, withdrawals, exchanges of currency, or other payments or transfers of US or foreign currency by, through, or to the financial institution in physical currency. Financial institutions must report cash-in or cash-out transactions of $10,000 or less that aggregate to in excess of $10,000 if they have knowledge, including knowledge from systems, that the transactions exceed $10,000. Banks, and only banks, may elect, but are not required to, exempt the transactions of certain customers if the requirements in regulations are followed.\textsuperscript{20}

Under parallel provisions in the BSA and the Internal Revenue Code and IRS regulations, other BSA financial institutions, insurance companies, and all other trades or businesses not subject to the BSA requirements for financial institutions must electronically file a FinCEN/IRS Form 8300 on cash in excess of $10,000 on any one day or in a series of related transactions during a rolling 12-month period. Under some circumstances, cash for reporting purposes can include not just US and foreign currency, but cash-equivalent monetary instruments, cashier’s and bank checks, traveler’s checks, and money orders with a face value of $10,000 or less.\textsuperscript{21}

Under both regulatory regimes, the failure to file a complete and accurate form or causing another person to fail to file a complete and accurate form, as well as the “structuring” of transactions to evade cash reporting requirements, can result in criminal and civil penalties, even if the funds involved in the transactions are derived from legal sources. Structuring involves the breaking down of amounts over $10,000 into transactions of $10,000 or less for the purpose of evading cash reporting requirements or the breaking down of transactions into amounts under $3,000 to avoid the funds transfer recordkeeping or monetary instrument recordkeeping requirements, discussed below.\textsuperscript{22}

b. **Suspicious Activity Monitoring and Reporting.** Banks, broker-dealers in securities, futures commission merchants and introducing brokers in commodities, mutual funds, insurance companies, most MSBs, casinos and card clubs, nonbank residential mortgage lenders and originators, and housing government-sponsored enterprises must electronically file Suspicious Activity Reports (SARs) with FinCEN if they know, suspect, or have reason to suspect that a transaction or attempted transaction by,
through, or at the financial institution involves money laundering or BSA violations i.e., structuring to avoid currency reporting or recordkeeping requirements; is unusual for the particular customer, with no known apparent legitimate business purposes; or involves the use of the financial institution to facilitate illegal activity e.g., financing terrorism with legitimately derived funds. There are parallel SAR regulations issued by the federal banking regulators that also require depository institutions to file SARs to report known or suspected violations of federal criminal law and to report insider abuse, but filing one SAR by a bank suffices to comply with both the FinCEN and banking regulator’s requirements.[23] Many states have parallel SAR requirements that also generally are satisfied by filing with FinCEN. Securities law violations required to be reported separately to a securities regulator or SRO generally would not also require filing a SAR.[24]

Generally, the reporting threshold is $5,000 ($2,000 for MSBs), with a $25,000 threshold for banks and broker-dealers for reporting known or suspected federal criminal violations that do not involve money laundering or BSA violations if the suspect is unknown (as in some credit card fraud schemes). There is no monetary threshold for known or suspected violations of federal criminal law by bank insiders.

Reports are required to be filed generally not later than 30 calendar days after initial detection of the facts that may constitute a basis for filing. This generally does not mean 30 days from identification of a possible red flag or computer alert for suspicion, but 30 days from the date when the financial institution knows or has reason to know that a transaction or the activity under review must be reported.[25] In matters requiring investigation, additional time may be needed to determine whether a transaction is suspicious, although the time spent investigating a potential suspicious transaction must be reasonable.[26] It is important to track and document every step in the SAR review and investigative process and to document decisions not to file. Care should be taken to complete the SAR fully and accurately, with all suspects listed and a full, but succinct, description in the narrative section of what transpired and why the financial institution believes it was suspicious.

Supporting documentation is not filed with the SAR, but it must be retained by the financial institution and made available to FinCEN or an
appropriate law enforcement agency upon request.

There are strict and detailed confidentiality rules with respect to SARs and SAR information. Financial institutions and their directors, officers, employees, and agents are prohibited under the BSA from advising anyone “involved in the transaction” that a report is being or has been filed. The BSA statute and regulations provide a safe harbor that protects financial institutions and their directors, officers, employees, and agents from liability under federal or state laws for filing a SAR or for failing to notify any person that a SAR has been filed. For instance, a banker would not be liable for defamation if the information in a SAR turned out to be wrong.\[27\]

Financial institutions must have a process in place that is reasonably effective to identify suspicious activity both at the time of the transaction through internal reports by alert employees and after the transaction has been completed by back-end risk-based monitoring. To manage the financial institution’s SAR reporting requirements, most financial institutions use automated transaction monitoring systems to help identify suspicious activity, which include case management tools to document the SAR decision-making process. These transaction monitoring systems employ rules and/or algorithms that look for red flags and anomalies in the transactional activities of their customers as measured against the customer profiles or customer peer groups. For these systems to work effectively, the rules must be tuned periodically to take account of any changes in the financial institution’s customer base, products and services offered, geographic locations, and money laundering schemes and the model validated. Many systems apply artificial intelligence based on what is known about customers and their transaction histories to identify potential suspicious activity. Specialized monitoring has been developed for certain business lines such as foreign correspondent banking.

In many financial institutions, investigation units or Financial Intelligence Units (FIUs) are in place to investigate possible suspicious activity identified by employees and, through monitoring, decide whether a SAR is required, and, if so, file the necessary SARs. Decisions not to file must be carefully documented. There may be supplemental monitoring by the business lines.

There is no safe harbor from criminal liability. Filing a SAR alone does not
insulate a financial institution from criminal liability for money laundering if the financial institution continues to conduct transactions with “knowledge” that the funds are from illegal activity.

It is critical to keep current with money laundering schemes in order to recognize and evaluate suspicious activity. Information about current money laundering methods and trends should be incorporated into the financial institution’s risk assessment and transaction monitoring system.[28]

In connection with fraud of all kinds, identity theft, mortgage fraud, telemarketing fraud, and cybercrime, it is important to remember that it is irrelevant to the SAR filing decision whether or not there has been a monetary loss to the financial institution. With the encouragement of FinCEN and the regulators, there has been a trend in some financial institutions to combine the fraud detection and prevention function with the BSA/AML function, or to closely coordinate the two functions. In some institutions, fraud prevention and suspicious activity reporting are the responsibility of a fraud or security department outside the BSA/AML compliance function. In these cases, the BSA officer should ensure that the policies, procedures, and internal controls governing identification, investigation, and decisions to file SARs by other areas of the institution are effective, well-documented, and result consistently in the timely filing of quality SARs.

1. **Reviews of Public Source Information and Other Risk Indicators.**
   Another source of potential red flags for suspicious activity is public source information (e.g., press and internet articles indicating that a customer may be involved in illegal activity); criminal subpoenas received by the financial institution for customer records; USA PATRIOT Act Section 314(a) and (b) requests, discussed below; or any inquiries from another financial institution about customers or transactions. Many institutions use commercial services to identify material negative news when an account is opened, periodically during the customer relationship and/or at set intervals depending on customer risk. The receipt of information from these sources alone does not allow or require a financial institution to file a SAR. The financial institution must independently conclude that suspicious activity was conducted by, through, or at the financial institution in order to be protected by the civil liability safe harbor. Nevertheless,
this external information serves as a red flag that a customer may have engaged in illegal activity and should trigger a review of the customer’s transactions to determine if any suspicious activity was conducted through the institution that may have been overlooked previously and now requires the filing of a SAR. Financial institutions that ignore these kinds of red flags could be exposing themselves to the risk of engaging in money laundering activity.

2. **Decisions to File SARs/Termination of Customer Relationships and Account Closings.** The BSA officer or his or her staff may—and should in some cases—consult with the business line to determine whether activity is suspicious. It is advisable that the decision whether to file a SAR, however, ultimately should be the decision of the BSA officer. There also should be a specific procedure providing for the review of an account or customer relationship if SARs have been filed or negative information is identified that raises concerns that the customer may have an illegal source of funds or may be using the financial institution for illegal purposes. The decision not to onboard a customer or to terminate a customer relationship can be made by the BSA officer alone, or there may be a formal consultative process with a recommendation from the BSA officer with input from a committee, including the BSA officer, the business line of the customer, and other appropriate areas of the financial institution. If a decision were made to retain a customer against the recommendation of the BSA officer, there should be an established escalation process within the financial institution to inform senior management and the board about the decision. This escalation process could be set forth in the AML policy and program document. The reasons for decisions to terminate or retain a customer should be well-documented. Once a decision is made to terminate a relationship, controls are needed to ensure that the necessary steps are taken to complete the severing of the relationship. In some cases, closing an account will require a notice period under the account agreement. Terminating loan relationships presents challenges, but if it is established that loan payments will come from an illegal source, the money laundering risk must trump financial loss.

FinCEN has issued guidance that, prior to closing an account where the financial institution is aware of a government investigation of the customer, law enforcement may request that the account be kept open.
for a period of time to facilitate a criminal investigation. These requests should be in writing, and the financial institution may want to consider requesting written protection from liability based on continuing to allow potentially suspicious activity to flow through the account.\[29\]

c. **Recordkeeping.** There are general recordkeeping requirements for all financial institutions and specific recordkeeping requirements for certain categories of financial institutions.\[30\] The record retention period generally is five years, including for records relating to the AML program; copies of all BSA reports filed and records relating to independent testing of the program; and BSA/AML training. Records must be maintained in a manner in which they are reasonably accessible upon a regulatory or law enforcement request. Unlike BSA reports, records maintained under the BSA generally only are accessible to law enforcement pursuant to legal process.

d. **Funds Transfer Recordkeeping and the “Travel Rule.”** Specific records are required to be retained relating to funds transfer of $3,000 or more by banks, broker-dealers, futures commission merchants and introducing merchants in commodities, mutual funds, casinos, and MSBs. What records are to be retained by the financial institution depend on the financial institution’s role in the funds transfer—whether the financial institution is the transmitter’s (originator’s) financial institution, an intermediary financial institution, or the recipient’s (beneficiary’s) financial institution.\[31\] In addition, under the Travel Rule, most of the information required to be recorded must “travel” in the transmittal order to the next financial institution in the payment chain.\[32\]

e. **Monetary Instrument Recordkeeping for Cash Sales.** Because monetary instruments are the equivalent of cash and figure in so many money laundering schemes, financial institutions that sell money orders, traveler’s checks, cashier’s checks, or bank checks are required to record the sales and verify the identity of persons purchasing these instruments in amounts of $3,000 to $10,000, inclusive.\[33\] Payments with groups of these instruments in amounts less than $3,000 may be an indication that they were purchased in transactions structured to avoid these requirements, and transactions in amounts under $10,000 may be an indication of structuring to avoid the CTR requirement.
f. **Customer Identification Programs.** Pursuant to an amendment to the BSA statute added by the USA PATRIOT Act and the implementing BSA regulations, banks, broker-dealers, futures commission merchants and introducing brokers in commodities, and mutual funds are required to develop a Customer Information Program (CIP) as part of their AML programs. FinCEN and the banking regulators also expect banks to impose CIP requirements on their operating subsidiaries. Under the CIP requirements, certain basic identification information must be recorded about customers (individuals and legal entities), and the identity of the customer must be verified through documentary means e.g., by review of a reliable and current government identification document, or by nondocumentary means. The CIP must describe the acceptable methods of identification and what must be done if identification cannot be verified satisfactorily. Records must be maintained of how identity was verified. Customers must be notified that customer identification information is required and that their identity will be verified. A model notification is included in the regulations.

The BSA regulations provide that, where two financial institutions subject to CIP requirements have a shared client (e.g., an introducing and clearing broker), they may enter a reliance agreement whereby only one of the financial institutions is responsible for CIP. If the regulatory requirements are followed, the relying financial institution receives a safe harbor from liability under the BSA if the other financial institution fails to perform its CIP responsibilities for any reason.

g. **Customer Due Diligence and Enhanced Due Diligence.** In May 2016, FinCEN published a final regulation that became effective on May 11, 2018, requiring certain financial institutions, banks, broker-dealers, future commission merchants and introducing brokers in commodities, and mutual funds to implement formal risk-based customer due diligence (CDD) programs that include certain minimum elements, including CIP, obtaining information about the nature and purpose of a customer’s account, ongoing monitoring of customer accounts, and obtaining beneficial ownership information at a 25% threshold for certain legal entity customers and identifying control parties (e.g., a chief financial officer).

In the past, risk-based CDD generally has not been a specific regulatory
requirement, but for many years, there has been a clear regulatory expectation that CDD—and for higher risk customers, enhanced due diligence (EDD)—will be a component of a risk-based AML program for financial institutions with account relationships. CIP is the first building block for CDD. The objective of CDD is not just to confirm the identity of the customer, but also to obtain adequate information and documentation about the customer and the customer’s sources of funds, and expected activity, to determine the risk that the customer may pose and to be able to monitor adequately the customer’s activity; i.e., to manage the risk and to comply with suspicious activity reporting and other BSA requirements. What information and documentation is obtained, what customer and related parties are subject to screening to identify politically exposed persons (PEPs) and material negative news, how frequently CDD/EDD information is updated, and what approvals are required to onboard high-risk categories of customer will depend on the risk rating of the customer. The FFIEC Manual is a good source of what customers generally should be subject to EDD; e.g., MSBs, PEPs, certain charities and nongovernment organizations (NGOs), and private banking customers.

Currently, CDD and EDD are by statute and regulation for only two categories of customers considered to pose a very high risk for money laundering: private banking accounts for non-US persons and foreign correspondent financial institution customers. These two requirements apply to “covered” US financial institutions under the regulations: banks, broker-dealers, futures commission merchants and introducing brokers in commodities, and mutual funds.

1. **Private Banking Accounts for Non-US Persons.** Under Section 312 of the USA PATRIOT Act and 31 C.F.R. § 1010.620, covered financial institutions are required to maintain due diligence programs with policies, procedures, and internal controls reasonably designed to detect money laundering through private banking accounts for non-US persons. The due diligence programs must include procedures to ascertain the identity of the nominal and beneficial owners of the account, the sources of funds deposited into the account, the purpose and expected use of the account, and whether any nominal or beneficial owner is a Senior Foreign Political Figure (SFPF). The procedures also must require reviews of the customer’s account activity to ensure that the activity is consistent with the information obtained and to identify and report any known or suspected money
laundering activity.

SFPFs, generally referred to as PEPs, are past or current senior foreign officials of any branch of government (including the military), senior major political party officials, and senior executives of foreign government-owned enterprises—and their close relatives, their close associates, and any legal entities owned by them or established for their benefit. The concern is that the funds of PEPs may be the proceeds of public corruption. Consequently, if a covered financial institution identifies a customer who is a PEP, enhanced due diligence must be conducted to ensure that the person’s funds are not the proceeds of public corruption.

With respect to PEP risk generally, not just for private banking, best practice is also to consider domestic (US) PEP risk.

2. **Foreign Correspondent Accounts.** Under Section 312 of the USA PATRIOT Act and the implementing BSA regulations, 31 C.F.R. § 1010.610, covered financial institutions that establish, maintain, administer, or manage a correspondent account for certain foreign financial institutions (foreign banks, broker-dealers, futures commission merchants, mutual funds, money transmitters, or currency exchangers) are required to establish a due diligence program. Under the program, the covered financial institution must assess the money laundering risk presented by each account based on a wide range of information about the foreign financial institution customer (e.g., the nature of its business and the markets that it serves, its owners, its anti-money laundering regulatory record, and the purpose and expected types and level of activities in the account). Covered financial institutions also should periodically update the information and review the account activity to identify suspicious activity.

In addition, enhanced due diligence must be conducted of certain high-risk foreign banks; i.e., banks operating under an offshore banking license and banks licensed by a foreign country that has been designated as noncooperative with international anti-money laundering principles by an intergovernmental organization or that has been designated as warranting “special measures” because of money laundering concerns by the Secretary of the Treasury, (this
h. **Prohibition on Correspondent Accounts for Shell Banks.** The USA PATRIOT Act added other amendments to the BSA addressed at money laundering through foreign financial institutions, especially in jurisdictions with lax AML controls. Under Section 313 and the BSA regulations—*31 C.F.R. § 1010.630*—banks, broker-dealers, futures commission merchants and introducing brokers in commodities, and mutual funds are prohibited from providing correspondent banking services directly or indirectly to foreign shell banks. Foreign shell banks are banks that are licensed by jurisdictions where they are not authorized to provide services (offshore licensed) and that have no physical presence in any country—no physical address, no employees, and no records—and that are not subject to inspection by the licensing authority. Banks that are affiliated with a regulated financial institution that maintains a physical presence; e.g., a UK bank with an offshore license in the Cayman Islands are not considered foreign shell banks. Foreign shell banks are effectively unregulated by any authority.

Banks and broker-dealers also are required to obtain ownership information about foreign correspondent account owners if the foreign financial institution is not publicly traded or has not filed a Form FR Y–7 with the Federal Reserve that identifies the current owners of the bank. Generally, information must be obtained about persons who own or control 25% or more of the voting shares of privately owned institutions.[37] Under Section 313(b), banks and broker-dealers also are required to obtain the name and address of a US agent for service of process for its foreign correspondent customers.

Banks and broker-dealers can obtain a safe harbor from liability under the shell bank and ownership information requirements if the foreign correspondent customer executes a Treasury form referred to as a USA PATRIOT Act Certification, and the US financial institution has no reason to believe the information is inaccurate. On the form, the correspondent customer certifies that it is not a shell bank and that it will not provide services indirectly to a shell bank through its account, certifies information about its ownership, and provides the name and address of its US agent for service of process. USA PATRIOT Act certification update forms are required to be executed every three years or sooner if any of the information changes.
i. **Section 311—Special Measures.** If designated to be of primary concern for money laundering, Section 311 of the USA PATRIOT Act authorized the Secretary of the Treasury to impose “special measures” on a foreign jurisdiction, one or more financial institutions in a foreign jurisdiction, or a class of transactions involving a foreign jurisdiction. The statute provides a range of measures that could be imposed on covered US financial institutions, including prohibitions on providing correspondent services to financial institutions in a designated jurisdiction or to a designated financial institution directly or indirectly through other correspondent accounts. Section 311 authority seems to be used to make a political point and, in some cases, to persuade a financial institution to change its ways. The authority has been used 25 times, mostly against specific financial institutions that have engaged in money laundering activities; e.g., terrorist financing or activities that have supported nuclear proliferation.

Special measures have been imposed through a rulemaking process, with a notice of proposed rulemaking followed by a final rule imposing special measures. Most covered financial institutions do not wait for a final rule to stop doing business with or processing transactions involving a financial institution where special measures are proposed. In some cases, the Section 311 designations have been rescinded without any final special measures having been imposed. The list of Section 311 actions and their current status is available from the FinCEN website.

j. **Section 314(a)—Government Information Sharing.** AML programs also must address compliance with the requirements of Section 314(a) of the USA PATRIOT Act and the related BSA regulations, 31 C.F.R. § 1010.520. Under Section 314(a), law enforcement agencies may refer names of persons (individuals or legal entities) suspected of money laundering or terrorism to FinCEN. FinCEN then will disseminate the list on the law enforcement agency’s behalf to financial institutions via a secure website and ask the financial institutions to respond via the same site whether they have accounts (or have had accounts in the last 12 months) for the persons on the list or have engaged in a certain transaction with the persons. While under the statutory and regulatory authority, FinCEN could send Section 314(a) requests to any financial institution subject to an AML program requirement, the requests currently are sent only to banks, broker-dealers, and certain large MSBs. The exact information about which financial institutions currently receive section 314(a) requests is not public. If the financial institution has a “hit,” law enforcement can then
direct a subpoena to the institution to obtain records relating to the person of interest.

Section 314(a) lists relate to ongoing investigations and are highly sensitive. Consequently, financial institutions are required to implement procedures to safeguard the confidentiality of this information, and it is expected by the regulators that the financial institution will limit the number of persons with access to the information.

k. **Section 314(b)—Voluntary Information Sharing Among Financial Institutions.** Under Section 314(b) and the implementing BSA regulations,[38] financial institutions subject to AML program requirements may elect to share information with each other about persons (individuals or legal entities) or countries for the purpose of identifying possible money laundering or terrorist activity. A financial institution that chooses to participate in Section 314(b) sharing is required to file an annual notice with FinCEN of its intention to share information that includes the name of the person within the institution to be contacted with requests. The form for the notice is available from the FinCEN website. Before making a Section 314(b) request of another financial institution, the requestor must take reasonable steps to verify that the financial institution has filed a notice with FinCEN, including by checking a list of Section 314(b) participants available from FinCEN. Financial institutions also must implement safeguards to ensure the confidentiality of the requests and the responses.

Information received under Section 314(b) only can be used to help identify or report money laundering or terrorist activities, determine whether to maintain an account or engage in a transaction, or assist a financial institution in complying with a BSA requirement. The regulations reinforce that, if the information provides a financial institution with information that gives rise to a SAR obligation, a SAR must be filed. There is a statutory and regulatory safe harbor from liability for violations of privacy laws for financial institutions that share information in strict compliance with the regulatory requirements.[39]

l. **MSB Registration.** Persons who own or control MSBs (except providers and sellers of prepaid access) are required to register and renew their registration every two years (or sooner if there is a change in ownership or control) with FinCEN by filing electronically a FinCEN Form 107 with
information about the MSB’s ownership, services, and locations.[40]

MSBs that are MSBs only because they are agents of another MSB; e.g., a Western Union agent or a sales agent for American Express traveler’s checks, do not need to register with FinCEN. MSBs that have agents are required to maintain lists of their agents (updated annually) with information specified in the regulations and provide the lists to FinCEN upon request.[41]

4. Designation of a BSA Compliance Officer.

The BSA officer should be designated as specified in the regulations or guidance, e.g., by the board of directors for banks and by senior management for securities broker-dealers and insurance companies, and where not specified (i.e., MSBs, casinos) at a similarly high level. The regulators expect the BSA officer to have adequate BSA experience and adequate authority within the organization to exercise effectively his/her responsibilities and be supported by adequate staff and systems. It is advisable that the compensation of the BSA officer and staff should be competitive to attract and retain well-qualified persons. The BSA function should be independent of the business lines; e.g., the BSA officer may report to the General Counsel or the head of the risk area. While BSA functions can be delegated, the BSA officer is responsible for compliance with the BSA requirements and should have the authority with respect to other areas of the institution that have BSA responsibilities. To the extent that business line, risk, or compliance staff support the BSA/AML function, but do not report to the BSA officer, it is advisable that the BSA officer have a role in their compliance review and compensation decisions.

5. Training and Communications.

BSA/AML training must be provided to all “appropriate” employees. There is a regulatory expectation that there be periodic training of the board and senior management. Generally, appropriate employees include employees who open accounts or establish other customer relationships, who have customer contact, who handle or review transactions, or who have BSA/AML compliance responsibilities; e.g., legal, compliance, risk, fraud, security, and audit personnel. Initial training should be provided to all appropriate personnel as soon as practical after an employee is hired, and refresher training should be provided periodically. A one-size training program does not fit all. While it
should suffice to provide general BSA/AML training to many employees, for other employees, especially those involved in high-risk lines of business or those with BSA/AML responsibilities, training will need to be tailored to the BSA/AML business line and responsibilities of the person being trained.

Currently, there is a trend to rely only on online training that includes a testing component. Online training can be effective, particularly for employees in low-risk business lines and with limited BSA/AML responsibilities, but for those in higher risk areas and those directly involved in BSA/AML functions, classroom training is often more effective. Persons with specific BSA/AML compliance functions, including BSA compliance personnel, lawyers who support the BSA/AML function, and auditors, should be exposed to external training opportunities and conferences.

Each financial institution should develop an annual training plan setting out who will receive training, the type of training, and when training should be completed. Records should be maintained of who received training, when, what material was covered, who conducted the training or how the training was provided, and the results of any testing. There should be disciplinary consequences for an employee who fails to complete training satisfactorily or who fails to attend training.

Training should be supplemented with timely communications and reminders from compliance and frequent reinforcement by management and senior management. Consideration should be given to including a discussion of money laundering in the institution’s ethics policy.


a. Independent Testing. Testing of the AML program must be independent in the sense that the persons who conduct the testing must be independent from the BSA compliance function.[42] Internal and external auditors or other qualified external consultants are permitted by the BSA to conduct the independent testing. Smaller institutions that rely on external consulting firms should conduct adequate due diligence to ensure that the firm is well qualified and has adequate BSA/AML experience. The frequency of the review may be set forth in regulations or guidance or, if not specified, should be based on risk. Auditors should be well trained on BSA/AML issues and the BSA/AML procedures and internal controls of the areas that they are testing.
It is advisable that auditors complete the same BSA/AML training required of the units that they are auditing. While all BSA/AML functions and aspects of the program should be tested, resources can be concentrated, and more time can be spent on high-risk accounts, transactions, and business lines or areas where there have been past audit or examination criticisms or recommendations. Information technology systems that support the BSA/AML functions also should be tested periodically.

BSA/AML independent testing results should be reported to the board or the audit committee of the board and to senior management and the management responsible for the area tested. The BSA officer should coordinate responses and remedial measures in response to audit and examination issues, criticisms, and recommendations, and report to appropriate management, senior management, and the board if remedial actions are not on track or appear insufficient.

Generally, it is a regulatory expectation that there be independent testing or validation of the completion and effectiveness of any remedial action taken in response to past audit or regulatory criticisms.

b. **Quality Assurance and Compliance Testing.** In addition to independent testing, in recent years, regulators have expected financial institutions to implement quality assurance procedures and compliance testing of the core BSA/AML functions, especially larger institutions. Unlike the audit function, personnel responsible for quality assurance can be part of the BSA/AML compliance function or can be in another area of the financial institution or in the business units. The overall quality assurance program should be risk based and be conducted in coordination with the BSA officer, and the results should be reported to the BSA officer and brought to the attention of appropriate management. The purpose of compliance testing, like independent testing, is to confirm that policies and procedures are being applied consistently and correctly and to identify problems or adjust procedures before there are major compliance deficiencies.

7. Other AML Program Considerations

a. **New Products and Services and Acquisitions.** Consideration should be given to having a written policy in place requiring the BSA officer to be involved in decisions to offer new products or services or to make significant changes in existing products or services. This can enable the BSA officer to
advise on the AML risk and on how to mitigate the risk and, in extreme cases, to advise management or the board that the risk cannot be managed.

Similarly, when a financial institution acquires another financial institution or the accounts of another institution, the BSA/AML risk of the acquisition should be considered and assessed to determine what further due diligence may be warranted upon acquisition and whether there are any gaps in the compliance program that should be addressed. In part with a view toward the risk of successor liability, the BSA officer should be in a position to advise senior management and the board on the acquisition and to help develop a plan to integrate the acquired institution into the financial institution’s AML program.

b. Use of Service Providers/Delegation of BSA Responsibilities. There are many situations where financial institutions outsource or delegate BSA functions to service providers who may be affiliated or unaffiliated with the institution. For instance, affiliated or unaffiliated transfer agents for mutual funds may be responsible for the mutual fund’s CIP and for monitoring transactions to identify suspicious activity. When BSA functions are delegated, the financial institution remains responsible for compliance and noncompliance under the BSA. Consequently, service agreements should specify carefully the BSA-related roles and responsibilities of the financial institution and the service provider. In addition, the financial institution should supervise the delegation and confirm that the service provider has the necessary training, procedures, controls, and systems to execute the delegated BSA responsibilities. The activities of the service provider should be subject to audit by the financial institution, and the service provider should be required to bring compliance lapses immediately to the financial institution’s attention.

c. Additional Considerations. Additional AML program considerations applicable to both financial institutions subject to BSA requirements and other businesses are discussed below.

Note on State Requirements

Many states have parallel money laundering criminal provisions and parallel anti-money laundering regulatory requirements for financial institutions that they license and regulate, e.g., state-licensed banks and MSBs, such as check
cashers and money transmitters. The requirements vary by state.

BSA Requirements Applicable to All Persons

In addition to cash reporting for all trades or businesses as defined in the IRS code discussed above, there are two BSA requirements that apply to all persons (individuals and legal entities), not just to financial institutions or financial businesses otherwise subject to the BSA.

Reports of Foreign Bank and Financial Accounts – FBARs

US persons with a financial interest in or signature or other authority over foreign bank, securities, and other financial accounts that, when aggregated, are valued over $10,000 at any point during the previous calendar year are required to file electronically an annual Report of Foreign Bank and Financial Accounts (FBAR)Form 114 with the IRS by April 15 of the following year. There are exceptions for certain persons with signatory authority for, but no financial interest in, foreign accounts—for instance, employees of a bank that is supervised by a bank supervisory agency who have signature authority over a foreign account by virtue of their bank employment. There is a pending rulemaking that will clarify the extent of the exception for persons with signatory authority, but no financial interest in foreign accounts.

FinCEN has delegated authority for FBAR administration and enforcement to the IRS. Unlike other BSA requirements, while FBAR requirements should be referenced in a financial institution’s AML program, responsibility for FBAR filing is usually with the financial institution’s tax or finance department rather than the BSA compliance area.

Cross-Border Monetary Instrument Reporting – CMIRs

Reports of International Transportation of Currency or Monetary Instruments (CMIR) are required when transporting, mailing, or shipping into or out of the United States, or receiving in the United States from outside the United States currency (US or the foreign equivalent) and/or other monetary instruments in excess of $10,000. For purposes of the CMIR requirement, “monetary instruments” include US and foreign currency, traveler’s checks in any form, incomplete negotiable instruments, and negotiable instruments or
securities in bearer form.\textsuperscript{[46]} There are certain exceptions for banks and broker-dealers, e.g., for shipments through the mail or by common carrier, but there is never an exception if a financial institution employee physically transports the currency or other monetary instruments into or out of the United States.

**Geographic Targeting Orders**

Under the BSA, if there is a demonstrated law enforcement need, FinCEN can impose “geographic targeting” — temporary regulatory requirements for financial institutions or other trades or businesses to file reports or keep records with certain characteristics for a set period of time.\textsuperscript{[47]} For instance, currently, under certain circumstances, there is a requirement in certain metropolitan areas for title insurance companies to report cash sales (nonfinanced sales) of real estate and at a given threshold amount.