Menu

Introduction
Suspicious Activity Reports
SAR Confidentiality
Five Key Components
Identifying the Suspicious Activity
Managing Alerts
Decision Making
Completion and Filing
Monitoring and SAR Filing on Continuing Activity
Wrap Up
Introduction

This course describes the BSA requirements for a bank to file a Suspicious Activity Report and why federal law limits sharing information about a SAR, and the components of a SAR monitoring and reporting system, and how to answer the essential questions that comprise the basis of the SAR narrative.

Current Version: 2.0

Last Update: September 2017. No substantial changes.

Last Review: September 2018. No changes needed.

Banks are required to report certain suspicious activities. Banks are also encouraged to report other possibly suspicious transactions which may be relevant to a possible violation of law or regulation. Suspicious transactions are those which may be intended to launder money, finance terrorist activities or connected to criminal activity. A suspicious transaction may also be one which apparently has no lawful purpose or which is extremely unusual for a particular customer and which has no reasonable explanation.

Suspicious activity reporting forms the cornerstone of the BSA reporting system. As indicated by its name, the activity that is reported by filing a Suspicious Activity Report (SAR) may not be criminal. It is a “suspicion” that something illegal may have happened and includes activity that raises a suspicion of illegal conduct or is otherwise unusual activity that lacks a business or apparent lawful purpose.

ABA course content does not provide, nor is it intended to substitute for, professional legal advice.
ABA course content does not provide, nor is it intended to substitute for, professional legal advice.
Introduction

SARs are intended to provide law enforcement with useful information. The information can be tips that illegal activity may be occurring or suspicious facts that may be combined with other information available to law enforcement to assist in the pursuit of a criminal case.

The information from SAR filings also supplies government agencies with the means to identify emerging trends and patterns associated with financial crimes. Accurate and timely information is critical to law enforcement agencies and so it is important that financial institutions ensure that SAR submissions are complete, sufficient, and timely.

Objectives

By the end of *BSA/AML: SAR Filing*, you will be able to

- Describe the scope of activities appropriate for SAR filing
- Discuss the importance of keeping SARs confidential
- Recognize some indicators of suspicious activity
- Describe the five key components of SAR filing
Suspicious Activity Reports

Money laundering
Banks are targets of money-laundering efforts because they provide ready access to the payment system and afford potential cover due to the large volume of daily transactions occurring at any given institution. As a result of the large volumes of daily transactions, individuals involved in money laundering may believe their laundering efforts will go undetected.

Federal investigators who try to stop money laundering find it a never-ending process. After they discover criminals’ latest money-laundering schemes, the criminals respond by creating even more inventive and complicated methods to launder money. These methods range from smuggling funds to the creation of intricate networks using wire transfers and shell companies.

Because the banking industry is also complicated and in a constant state of change, law enforcement officials and bankers face a huge challenge identifying and investigating money laundering. The process of tracking the money is tedious and lengthy because investigators are dealing with the continuous changes and complexities of new money-laundering schemes and the banking industry.

Glossary term:
Shell companies
The term “shell company” generally refers to a business entity with no significant assets or ongoing business activities. Shell companies—formed for both legitimate and illicit purposes—typically have no physical presence other than a mailing address, employ no one, and produce little to no independent economic value. Shell companies often can be used in money-laundering operations.
Suspicious Activity Reports

A bank is required by federal regulations to file a completed SAR by sending the report to FinCEN in the following circumstances involving criminal violations:

- Insider abuse of any amount
- $5,000 or more where a suspect can be identified
- $25,000 or more regardless of potential suspects

In addition, a bank must file a SAR on transactions conducted or attempted which total $5,000 or more if the bank suspects or has reason to suspect that the conduct displays the following characteristics:

- Involves possible money laundering or illegal activity
- Is designed to evade the BSA
- Has no business or apparent lawful purpose OR is not the type of transaction the customer would ordinarily engage in

Note: A bank is not required to file a SAR for a robbery or burglary that is reported to appropriate law enforcement officials.
Suspicious Activity Reports

If you, as a bank employee, encounter suspicious transactions that may relate to terrorist activity, notify the appropriate person at your bank immediately.

FinCEN maintains a FINANCIAL INSTITUTIONS HOTLINE that operates 7 days a week, 24 hours a day to facilitate the immediate transmittal of this information to law enforcement. This HOTLINE provides law enforcement and other authorized recipients of Suspicious Activity Report (SAR) information with details of the suspicious activity in an expedited fashion.

Using the HOTLINE is voluntary and is not a substitute for an institution’s responsibility to file a SAR in accordance with applicable regulations.
Insider abuse
What is “insider abuse” for the purposes of SAR filing? The term “insider abuse” is not defined in the BSA but appears in SAR rules issued by Federal financial regulators.

For SAR purposes, “insiders” can be directors, officers, employees, agents or other individuals affiliated with the bank who may have committed or aided in the commission of a criminal act. Whenever an insider is involved, a SAR must be filed regardless of the amount involved.

Insiders are generally individuals who hold a position of trust in the institution or who are closely affiliated with it and who have, in general terms, breached their fiduciary duties; traded on inside information; usurped opportunities or profits; engaged in self-dealing; or otherwise used the institution for personal advantage.

» Click the image to see possible examples of insider abuse.

Possible examples of insider abuse may include the following actions:

- Using institution funds for personal vacations or to buy personal automobiles, clothing, and art
- Payment of consulting fees to insiders or their companies
- Putting friends and relatives on the payroll of the institutions
- Teller theft from a cash drawer or vault, often followed by forced balancing
- Opening new accounts for fraudulent or non-existent customers to qualify for performance goals or employee incentive programs
- Improperly crediting back overdraft fees and other service charges to themselves and others

Glossary term:

Institution-affiliated party
Any director, officer, employee, or controlling stockholder (other than a bank holding company) agent, shareholder, independent contractor (including attorney, appraiser, or accountant) who knowingly or recklessly participates in the conduct of the affairs of an insured depository institution.
Safe harbor

The safe harbor protects bank employees so that they will not fear or hesitate to report suspicious or unusual activity to the designated individual at your bank. All employees are encouraged to report any and all suspicious activity identified in the course of conducting their day-to-day work. It may be that, after an in-depth investigation, a decision will be made by the official in charge not to file a SAR, but this should not discourage you or any bank employee from advising your BSA officer or other designated individual at the bank of your suspicions or uncertainty about unusual activity.

Suspicious Activity Reports

Safe harbor

The safe harbor protects bank employees so that they will not fear or hesitate to report suspicious or unusual activity to the designated individual at your bank. All employees are encouraged to report any and all suspicious activity identified in the course of conducting their day-to-day work. It may be that, after an in-depth investigation, a decision will be made by the official in charge not to file a SAR, but this should not discourage you or any bank employee from advising your BSA officer or other designated individual at the bank of your suspicions or uncertainty about unusual activity.
Suspicious Activity Reports

Persons involved in money laundering or other types of financial crime are often aware of the reporting requirements of the BSA and will try to get around the law whenever possible. It is critical, therefore, for bank employees to know their customers and the type of transactions they normally conduct. In addition to the required SAR reporting thresholds, a bank can file a SAR anytime regardless of the dollar amount if the bank feels law enforcement could benefit from the information. Any transactions that seem out of place or unusual and cannot be reasonably explained by a legitimate business reason should be reported according to bank policy.

Aside from unexplained suspicious activity that may indicate money laundering, human trafficking or smuggling, or even terrorist financing, the SAR process is also intended to detect and report activity that constitutes more direct types of financial crimes such as credit card fraud, identity theft, check kiting, and insider abuse—just to name a few.
Suspicious Activity Reports

Self Check Quiz

In which three circumstances is a bank required by federal regulations to file a completed SAR by sending the report to FinCEN?

» Select the correct answers and click Submit.

- A) Insider abuse of $5,000 or more
- B) Insider abuse of any amount
- C) $5,000 or more where a suspect can be identified
- D) $25,000 or more regardless of potential suspects

B, C, and D are correct.
A is incorrect because a bank is required by federal regulations to file a completed SAR for insider abuse of any amount.
SAR Confidentiality

Because the information in a SAR is only an unproven suspicion, and to encourage banks to share information about possible criminal or terrorist activity with law enforcement, federal law strictly limits the ability to share information about a SAR or the SAR itself.

The general rule: No institution, director, officer, employee, or agent of a bank that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. In addition, other bank employees should only be informed on a “need to know” basis.

Institutions must be vigilant in maintaining the confidentiality of SARs. This includes ensuring all employees, agents, and individuals appropriately entrusted with information in a SAR are informed of the individual obligation to maintain SAR confidentiality. This obligation applies not only to the SAR itself, but also to information that would reveal the existence (or non-existence) of the SAR. Likewise, such persons should be informed of the consequences for failing to maintain such confidentiality, which could include civil and criminal penalties.

Page 10
SAR Confidentiality

The unauthorized disclosure of a SAR is a violation of federal law. Both civil and criminal penalties may be imposed for SAR disclosure violations. Violations may be enforced through civil penalties of up to $100,000 for each violation and criminal penalties of up to $250,000 and/or imprisonment not to exceed five years.

In addition, financial institutions could be liable for civil money penalties resulting from anti-money laundering program deficiencies (i.e., internal controls, training, etc.) that led to the SAR disclosure. Such penalties could be up to $25,000 per day for each day the violation continues. Incidents involving possible unauthorized SAR disclosures are investigated, and appropriate action is taken for violations of the law.

If subpoenaed or requested to disclose a SAR or information contained in a SAR, a bank employee must decline to produce the SAR and decline to provide any information that would disclose that a SAR has been prepared or filed. FinCEN and the bank’s primary banking regulator must be notified about the request.

Warning: NEVER discuss a SAR with customer or even inform him or her that you are filing the report. This is different from the rules on currency transaction reports (CTRs), which may be discussed with customers if your bank allows you to have such discussions.
BSA/AML: SAR Filing

SAR Confidentiality

Exceptions
There are times, though, when it is appropriate to share a SAR or information about a SAR filing, but they are extremely limited and must be handled carefully. If there are any questions, you should contact your bank’s BSA officer.

A SAR may be shared with the following entities:

- FinCEN or any federal, state, or local law enforcement
- Any federal or state regulatory authority that examines the bank for compliance with the BSA
- Another financial institution, the underlying facts, transactions, and supporting documents of a SAR may be disclosed to another financial institution for the preparation of a joint SAR, or in connection with certain employment references or termination notices as authorized by the BSA
- Head offices and affiliates, the sharing of a SAR by a bank or its agent with certain permissible entities within the bank’s corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act is also allowed. Institutions may share SARs with the head offices, companies under common control and controlling companies, whether in the U.S. or abroad. This promotes compliance with the applicable requirements of the BSA by enabling the head office or controlling company to discharge its oversight responsibilities with respect to enterprise-wide risk management, including oversight of a bank’s compliance with applicable laws and regulations

Glossary terms:

Common control
Under “common control” means that another company, directly or indirectly, or acting through one or more other persons, owns, controls, or has the power to vote 25 percent or more of any class of the voting securities of the company and the depository institution or controls in any manner the election of a majority of the directors or trustees of the company and the depository institution.

Controlling company
A “controlling company” is defined as a bank holding company (BHC).
SAR Confidentiality

Because foreign branches of U.S. banks are regarded as foreign banks for the purposes of the BSA, they are affiliates that are not subject to a SAR regulation. Accordingly, a U.S. bank that has filed a SAR may not share the SAR, or any information that would reveal the existence of the SAR, with its foreign branches. Banks should maintain appropriate arrangements with head offices, controlling companies, and affiliates to protect the confidentiality of SARs. The bank should have policies and procedures in place to protect the confidentiality of the SAR as part of their internal controls.

Your BSA officer also is expected to notify the bank’s board of directors or an appropriate board committee of the board about the bank’s SAR filings. There is no mandated format or frequency; reports may be made monthly or quarterly or even less often depending on the volume of SARs filed. The BSA officer must stress the confidential nature of SAR data when providing information to the board.

**Note:** Only authorized personnel such as the bank’s BSA officer can make the determination regarding information sharing. Other bank personnel who know of the existence of a SAR should never take it upon themselves to share such information, even if requested to do so by law enforcement.
SAR Confidentiality

Question:
Because the information in a SAR is only an unproven suspicion, federal law strictly limits the ability to share information about a SAR or the SAR itself. With which entities outside of the bank may SAR information be shared?

Answer:
A SAR may be shared with the following entities:

- FinCEN or any federal, state, or local law enforcement
- Any federal or state regulatory authority that examines the bank for compliance with the BSA
- Another financial institution; the underlying facts, transactions, and supporting documents of a SAR may be disclosed to another financial institution for the preparation of a joint SAR, or in connection with certain employment references or termination notices as authorized by the BSA
Five Key Components

Generally, effective suspicious activity monitoring and reporting systems include five key components. These components, listed below, are interdependent and an effective suspicious activity monitoring and reporting process should include successful implementation of each component. Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA compliance.

An effective SAR monitoring and reporting system consists of the following five key components:

1. Identifying the Suspicious Activity
2. Managing Alerts
3. Decision Making
4. Completion and Filing
5. Monitoring and SAR Filing on Continuing Activity

Suspicious activity monitoring and reporting are critical internal controls since proper monitoring and reporting processes are essential to ensure that the bank has an adequate and effective BSA compliance program.

The bank should have appropriate policies, procedures, and processes to monitor and identify unusual activity. The bank’s risk profile will determine the sophistication of monitoring systems. These systems should pay particular attention to products, services, customers, entities, and geographies which present greater risk for money laundering, terrorist financing, or other financial crimes.

The bank should ensure adequate staff is assigned to identify, research, and report suspicious activities. In making these determinations, management will take into account the bank’s overall risk profile and the volume of transactions. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

For more information on risk assessment, refer to the BSA/AML: Risk Assessment and Customer Due Diligence Frontline course.

---

| Page 15 |
1. Identifying the Suspicious Activity

Banks must report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and other crimes that exceed the regulatory dollar thresholds. While banks are required to report suspicious activity, banks are not required to confirm the underlying crime. Investigation is the responsibility of law enforcement. However, when evaluating a suspicious activity and filing a SAR, it helps law enforcement when a bank identifies the specific characteristics of the suspicious activity. This is one reason that banks assign the responsibility to one person or division to make the decision. However, when evaluating suspicious activity and completing the SAR, banks are expected, to the best of their ability, to identify the characteristics of the suspicious activity.

Unusual activity identification can result from the following sources:

- Employee identification
- Law enforcement requests (including National Security Letters)
- Transaction monitoring
- Surveillance monitoring

Page 16
1. Identifying the Suspicious Activity

Employee identification
Employee identification includes suspicious activities which are identified by employees during day-to-day operations. Therefore, employees need methods they can use to report suspicious activity to the appropriate personnel within the bank, such as a worksheet, e-mail, or phone. Some banks ask employees to report to supervisory staff while others provide a central point of contact.

It is hard to say what suspicious activity "looks like." Suspicious activity will appear differently based on what role you have at the bank and how you interact with customers. For example, a teller might identify certain activity as being suspicious that a lender may never see, such as structuring of deposits to avoid CTR reporting. The opposite is also true, since a lender will be able to identify suspicious activity that a teller would not see, such as fraudulent information on loan applications. This is one of the reasons that it is important not only to know your customers but to ensure that all bank employees are trained to recognize suspicious activity when it occurs.
1. Identifying the Suspicious Activity

Employee identification—Tellers and CSRs
A typical example of a suspicious transaction for a teller is when a customer begins to conduct a currency transaction which exceeds $10,000 but then reduces the amount of the transaction to stay below $10,000 when told that a CTR must be completed for large cash transactions. Variations of this situation, referred to as structuring, are perhaps the most frequently cited examples of suspicious transactions that occur in banks.

» Click the image to see a list of examples of suspicious activity that may come to the attention of a teller or CSR.

Suspicious activity examples
- Corporate accounts where deposits or withdrawals are primarily in cash rather than checks
- Small businesses that frequently make cash deposits consisting of $50 bills and/or $100 bills
- Single-location businesses that make deposits at several branches of your bank
- Customers who frequently visit their safe deposit boxes before making cash deposits that are always less than the reportable dollar amount
- Deposits of sequentially numbered cashier’s checks or money orders
- Large amounts of cash deposited that are wrapped with the currency straps from another bank
- Customers who insist on being added to the bank’s CTR exemption list
- Customers who make numerous, separate deposits at ATMs below the reportable dollar amount
- Customers who are reluctant to provide personal information or information about their businesses
- Customers who have no record of past or present employment but make frequent large transactions
- Customers whose activity is inconsistent with their business
- Accounts receiving multiple ACH payroll deposits for individuals not on the account (may indicate human trafficking)

» Click the image of Krystal Ball to see a suspicious activity scenario.

Example
Krystal Ball, a customer of First National Bank, brought $27,000 in cash to deposit to her checking account. When the teller told her she would need to complete a CTR, she took back the money and left the bank (refusing to complete a transaction is suspicious and may be sufficient reason to file a SAR). The next day, there were three separate cash deposits into Krystal’s checking account of $9,000 each, apparently to avoid the CTR filing. Besides splitting the deposit into smaller amounts, a step known as structuring, two of the deposits were made by Krystal’s son and nephew at different First National Bank branches.
In this example, the bank would still need to aggregate (add together) the transactions conducted in one business day and file a CTR, but the attempt to structure the transactions could also require the bank to file a SAR.

Glossary term:

**Structuring transactions**
A person structures a transaction if that person conducts or attempts to conduct one or more transactions in currency in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the CTR filing requirements. “In any manner” includes, but is not limited to, breaking down a single currency sum exceeding $10,000 into smaller amounts that may be conducted as a series of transactions at or less than $10,000. The transactions need not exceed the $10,000 CTR filing threshold at any one bank on any single day in order to constitute structuring. Structuring is covered in more detail in the *BSA/AML: Overview* Frontline course.
1. Identifying the Suspicious Activity

Employee identification—Lenders
Suspicious activity detection and monitoring at financial institutions should be an enterprise-wide process that considers the entire customer relationship. While an institution may have a sound process to identify and monitor potentially suspicious activities in deposit account products, formal processes may not exist for the institution’s loan accounts. Monitoring a customer’s entire relationship can give bankers greater perspective on the legitimacy and legality of a customer’s business and transactions, especially when it comes to the lending function.

Bank employees involved in the lending function will encounter numerous situations that could be considered suspicious.

Example
Larry Sprinkle, the local TV weatherman and a customer of First National Bank, has applied for a loan. He has never married, preferring to devote himself entirely to predicting the weather. Mr. Sprinkle tells the loan officer that he is in danger of being replaced at WJRK TV by Jerry Storm, a local celebrity tornado chaser, but Larry thinks if he can upgrade his education and becomes certified in weather forecasting, he can hold on to his job. According to the loan application, the funds will be used to obtain a certification from the American Meteorological Society.

In looking at his financials, it does not appear that Larry’s income supports the amount he wants to borrow. Larry also exhibits a lavish lifestyle that is not supported by the income from his job. Larry has offered several recently purchased CDs as collateral for the loan but the source of the funds in those CDs is unclear and appears to have come from multiple negotiable instruments deposited to Larry’s account by unknown persons.
1. Identifying the Suspicious Activity

Employee identification—Lenders, continued

Due diligence is required during the loan application and underwriting process through Customer Identification Procedures (CIP) and loan documentation requirements. However, the level of customer due diligence (CDD) performed for guarantors, signatories, principals, and other loan participants can vary, in part due to the fact that CIP compliance may not be required for some of these individuals.

One of the most important controls to address this aspect of compliance is the bank’s BSA/AML training program. The bank’s training program should provide for role-specific training and educate bank personnel on the types of activity that are deemed suspicious in their particular area of the bank.

The objective of CDD should be to help the bank predict with relative certainty the types of transactions that will be typical for a particular customer. These processes also should help the bank determine when transactions are potentially suspicious.

» Click the image to see examples of unusual activities lenders might see that may warrant follow up consideration.

- Unusual activity examples
  - A customer presents documents that cannot be readily identified or verified
  - A customer provides both an ITIN and a SSN
  - A customer’s home or business phone is disconnected for no apparent reason
  - A customer is a trust, shell company, or private investment company that is reluctant to provide information on controlling parties or underlying beneficiaries
  - A customer does business in high-risk locations
  - A customer offers bribes to the loan officer for overlooking certain discrepancies
  - A customer provides false or conflicting identification

While loans secured by cash collateral and/or marketable securities are typically considered lower risk credits, they can easily be used to hide illegal monies or to obscure the purpose of funds. This is not the only way loans are used to launder money, but this is one of the most common methods. The fact is, any loan can be used to launder money, but understanding the red flags and educating personnel on how to evaluate and monitor loan customers can help to mitigate BSA/AML risk.
1. Identifying the Suspicious Activity

Employee identification—Mortgage lenders
Depository institutions have seen a large increase in mortgage loan fraud. According to the FBI, mortgage fraud continues to be an escalating problem in the United States. The FBI also reports that many borrowers across the U.S. are still struggling with their mortgages, which creates an ideal climate for mortgage fraud perpetrators to employ a variety of schemes. Emerging and re-emerging schemes include loan modification scams, foreclosure rescue, and identity thefts exploiting home equity lines of credit.

In recent years federal and state law enforcement and regulatory agencies have devoted considerable effort to the prevention, investigation, and prosecution of mortgage loan fraud. One of the ways law enforcement becomes aware of mortgage fraud is through the analysis of SARs filed by banks. These SARs provide valuable intelligence in mortgage fraud trends and can lead to the initiation of mortgage fraud cases as well as the enhancement of law enforcement investigations.

» Click each image below to learn more about loan fraud.

Common types of mortgage fraud
According to FinCEN, the following are common types of mortgage fraud:

- **Income fraud:** Includes both overstating income to qualify for larger mortgages and understating income to qualify for hardship concessions and modifications
- **Appraisal fraud:** Includes both overstating home value to obtain more money from a sale of property or cash-out refinancing and understating home value in connection with a plan to purchase a property at a discount to market value
- **Liability fraud:** Occurs when borrowers fail to list significant financial liabilities, such as other mortgages, car loans, or student loans, on mortgage loan applications. Without complete liability information, lenders cannot accurately assess borrowers’ ability to repay debts
- **Foreclosure rescue scams:** Targets financially distressed homeowners with fraudulent offers of services or advice aimed at stopping or delaying the foreclosure process. Some of these scams require homeowners to transfer title—or make monthly mortgage payments—to the purported “rescuer,” rather than the real holder of the mortgage. Some foreclosure rescue scams require homeowners to pay fees before receiving “services,” and are known as “advance fee” schemes
BSA/AML: SAR Filing

- **Social Security number (SSN) fraud and other identify theft**: Includes the use of an SSN or other government identification card or number that belongs to someone other than the applicant in a loan application. Identity theft includes broader use of another’s identity or identifiers (beyond an SSN) to obtain a mortgage or perpetrate a “fraud for profit” scheme.

**Red flags for mortgage loan fraud**

- Inflated appraisals
- Bonuses to brokers or fee-based providers paid outside of closing or at closing
- Higher fees than customary for the local market
- Falsifications of income, deposits, rents, etc.
- Falsifications of identity documents—ITINs and SSNs for the same person
- Fake supporting documentation
- Requesting documents be signed in blank
- Purchase loans disguised as refinancings with cash outs
- Investment opportunities and guarantees
- Terms too good to be true
- High pressure tactics employed
- Unexplained excessive fees/costs
- Requiring “prepayment” of certain disallowed fees
1. Identifying the Suspicious Activity

Identifying suspicious activity—All bank employees

The use of legitimate funding sources for terrorist objectives is a form of financial crime that often defies detection. One key difference between terrorists and traditional criminal organizations is that terrorist organizations often use funds from legitimate sources to support their objectives.

Terrorists are usually motivated by ideological and political goals unlike other criminals who are motivated by profit. For the terrorist, money is a means to an end while for other criminals the money is an end in itself. Therefore, terrorists may use funds that come from legitimate sources while money launderers have funds from illegitimate sources that they are trying to make appear legitimate.

In addition to using funds from legitimate sources, terrorists often engage in illegal activity, like kidnapping or human trafficking, to earn money to support their terrorist goals. Other funding sources for terrorists can include extortion, narcotics trafficking, smuggling, fraud, identity theft, and improper use of charitable donations. However, the fact that terrorists often rely on legitimate funds can make it extremely difficult to distinguish a transaction that supports terrorist activities from normal bank transactions; for example, the 9/11 hijackers withdrew funds from ATMs that were no different from withdrawals by any other consumer.
1. Identifying the Suspicious Activity

Identifying suspicious activity—All bank employees, continued

Financial institutions should develop practices and procedures to help detect transactions that may involve funds used in terrorist financing so that the bank is not used unknowingly to further the goal of terrorism. To do this, banks should be aware of possible red flags that could indicate funds involved in terrorist financing.

The following categories of potentially suspicious or unusual activities help show examples of transactions that could be a reason for additional scrutiny. These categories and examples are not exhaustive, but should be used with other available information (including any lists of suspected terrorists, terrorist groups, and associated individuals and entities issued by appropriate national authorities), the nature of the transaction, and the parties involved in the transaction. While any one or more of the factors listed may warrant further investigation, none of these factors by itself means the transaction is suspicious or unusual.

» Roll over each category to see examples of potentially suspicious or unusual activities.

Accounts
- Accounts that receive periodic deposits but then stay dormant. These accounts can be used to create a legitimate appearing financial background through which additional fraudulent activities may be carried out.
- A dormant account with a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.
- When opening an account, a customer refuses to provide information, attempts to reduce the level of information provided, or provides information that is misleading or difficult to verify.
- An account for which several persons who are unrelated or have no apparent connection have signature authority.
- An account opened for a legal entity or organization using the same address as other legal entities or organizations, where the same person or persons have signature authority, but there is no apparent economic or legal reason for such an arrangement.
- An account opened in the name of a recently formed legal entity where a higher than expected level of deposits are made in comparison with the income of the founders of the entity.

Funds transfers
- A large number of incoming or outgoing funds transfers through a business account without any logical business or other economic purpose for the transfers. This is especially true when the activity involves higher-risk locations.
- Funds transfers that do not include information on the originator or the person on whose behalf the transaction is conducted when the inclusion of such information would be expected.
BSA/AML: SAR Filing

- Foreign exchange transactions for a customer that are conducted by a third party followed by funds transfers to locations that either have no apparent business connection with the customer or that are higher-risk countries

**Deposits and withdrawals**
- Large cash withdrawals from a business account not normally associated with cash transactions
- Large cash deposits to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted by check
- Multiple transactions on the same day at the same branch of a financial institution with an apparent attempt to use different tellers
- Structuring of deposits through multiple branches of the same financial institution or by groups of individuals who enter a single branch at the same time
- Deposit or withdrawal of cash in amounts which fall consistently just below identification or reporting thresholds
- Deposit or withdrawal of multiple monetary instruments at amounts which fall consistently just below identification or reporting thresholds, particularly if the instruments are sequentially numbered

**Characteristics of the customer and/or the customer’s business activity**
- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (for example student, unemployed, self-employed, etc.)
- Stated occupation of an account holder or transactor which is not consistent with the level or type of activity in the account or transaction—for example, a student or unemployed individual who receives or sends large numbers of wire transfers or who makes daily maximum cash withdrawals at multiple locations over a wide geographic area
- Financial transactions by or for non-profit or charitable organizations with no logical economic purpose or where there is no link between the stated activity of the organization and the parties in the transaction
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer does not appear to justify the use of a safe deposit box
1. Identifying the Suspicious Activity

Exercise

Situation 1

Background
Betty A. Warren, a teller at the Last Bank of the South, notices an increase in cash withdrawal activity from an account owned by Misty Smith, a contract law attorney. These large cash withdrawals, just under the $10,000 reporting threshold for CTR filing, appear to follow the deposit of sequentially numbered money orders and cashier’s checks. This activity seems very unusual for a contract law attorney and Misty has not transacted business in this way in the past. Betty has a long line of customers waiting. Because Misty is an established customer, and because Betty is in such a hurry to get to the other customers, Betty makes the decision to overlook reporting Misty’s transactions to management.

What would you have done if you were Betty?

» Type your answers in the field. When finished, click the Suggested Results button to view possible responses.

Suggested Results

Betty should not ignore the activity. Betty could be missing a very important opportunity to protect the bank and failure to report the activity could cause Betty to be accused of “willful blindness.” Willful blindness is deliberate failure to make a reasonable inquiry of wrongdoing despite suspicion or an awareness of the high probability of its existence. Willful blindness involves conscious avoidance of the truth and gives rise to an inference of knowledge of the crime in question.

Although there may be a very logical and legal reason for the unusual activity, Betty is in no position to know that. Betty does not have to refuse to conduct Misty’s transactions, nor close her line down and ignore other customers. However, when she gets an opportunity, she should report the activity to the bank’s BSA officer or whoever is responsible for filing SARs. After investigating the activity, the bank may decide not to file a SAR, but that is a decision that should be made by the appropriate person at the bank.
Exercise

Situation 2

Background
Helen Wailing is a loan officer at the Third National Bank. Krystal Morgan applies for a loan to purchase a pickup truck. When Helen obtains Krystal's credit report, it contains an identity theft alert and an address discrepancy alert. Krystal says she placed the alert because someone hacked the database of the university she attended and all students were advised to place such an alert. She says the address discrepancy is due to the fact that her husband abandoned her and their 7 kids she had to move into an apartment, but the credit report still shows the house as her primary residence.

Things have been really slow in the auto lending department lately and Helen has had a hard time meeting her goals. Helen feels that she can rely on her 40 years of experience as a loan officer, and believes that the explanations that Krystal has provided for the alert and the address discrepancy all sound reasonable.

What would you do if you were Helen?

Type your answers in the field. When finished, click the Suggested Results button to view possible responses.

Suggested Results
Helen should not ignore the obvious suspicious issues with this loan. Although Krystal may be telling the truth, Helen is in no position to make a loan knowing that information given is potentially fraudulent or may have been obtained as a result of identity theft. Therefore, further investigation is needed before a decision can be made.
1. Identifying the Suspicious Activity

Self Check Quiz

Bill Stodder is the owner of a delicatessen near the bank. He frequently makes large cash deposits to his general operating account at your bank. Which two options might lead you to believe this activity is suspicious?

» Select the correct answers and click Submit.

- A) Bill always comes to the bank at 3 p.m.
- B) Bill repeatedly makes deposits consisting of moldy-smelling $50 and $100 bills
- C) It is unusual for a deli to make large cash deposits
- D) Bill is very friendly

B and C are correct.
A is incorrect because the fact that he comes to the bank in the afternoon could just indicate that he does his banking after the lunch rush. D is incorrect because the fact that he is friendly does not indicate suspicious activity.
Self Check Quiz
Which three customer situations could indicate suspicious activity?

Select the correct answers and click Submit.

- A) Customer presents unusual documents that cannot be readily identified or verified
- B) Customer's home or business phone has been disconnected for no apparent reason
- C) Customer provides both an ITIN and a SSN
- D) Customer has a single location business that makes deposits at only one branch of your bank

A, B, and C are correct.

D is incorrect because individuals wishing to conduct illegal activity will take deposits to different branch locations hoping the bank will not have the ability to aggregate all of the activity if it is done in different locations.
1. Identifying the Suspicious Activity

Law enforcement inquiries and requests

The following examples of law enforcement requests are another way banks may be alerted to potential suspicious activity:

- Grand jury subpoenas
- **National Security Letters (NSL)**
- **314(a) requests**

Each bank should establish policies and procedures for the following tasks:

- Identifying the subject of the request
- Monitoring their transaction activity if appropriate
- Identifying potentially suspicious activity, and as appropriate, filing a SAR

It is important to understand that a grand jury subpoena, an NSL, or a 314(a) request alone does not mean that something is suspicious. Law enforcement or the grand jury may be seeking information for an investigation that is not directly related to the bank’s own customer. However, it may be a reason to investigate further.

**Note:** Due to the confidentiality of grand jury proceedings, if a bank files a SAR after receiving a grand jury subpoena, law enforcement discourages financial institutions from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Instead, the SAR should reference only the facts and circumstances that supported the finding of suspicious activity.

Glossary terms:

**National Security Letters**

National Security Letters (NSLs) are written investigative demands that may be issued by local FBI and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain records from financial institutions. These are highly confidential and must be handled following all appropriate procedures.

**314(a) request**

A 314(a) request is an information sharing procedure authorized by section 314(a) of the USA PATRIOT Act. Section 314(a) authorizes a federal, state, local, or foreign law enforcement agency investigating terrorism or money laundering to request that FinCEN solicit, on its behalf, certain information from banks and other financial institutions about an individual, entity, or organization about which the law enforcement entity is seeking information.
1. Identifying the Suspicious Activity

National Security Letters are also highly confidential, so no financial institution or officer, employee, or agent of the institution, can disclose to any person that a government agency has sought or obtained access to records through an NSL.

The BSA officer must take appropriate measures to ensure confidentiality and the bank should have written policies and procedures in place for processing and maintaining confidentiality. If a SAR is filed, it should not contain any reference to receipt or existence of an NSL and should only reference the facts and activities that supported the decision to file a SAR.
1. Identifying the Suspicious Activity

There are two processes that help the bank identify suspicious activity: transaction monitoring and surveillance monitoring. Depending on the size and risk profile of your bank, the bank may use one or both of these systems.

**Transaction monitoring**
Transaction monitoring is a process used by banks for reviewing types of transactions for potentially suspicious activities. It can be manual but increasingly, banks are taking advantage of software programs to handle the monitoring. When the monitoring is done by software, the bank must review the reports generated by the system which identify potentially suspicious activity.

The following reports are examples of those used in monitoring:

- Cash, Wire, or Monetary Instrument Sales reports
- Significant Balance Change reports
- Nonsufficient Funds (NSF) reports
- Structured Transaction reports
1. Identifying the Suspicious Activity

» Roll over the reports below to see some of the information generated by transaction monitoring reports.

Currency activity reports

Currency activity reports are used to help the bank file Currency Transaction Reports and identify suspicious cash activity. These reports include the following information:

- Cash transactions, either deposits or withdrawals, aggregating $10k or more and therefore requiring a CTR
- Cash transactions (either single or multiple transactions) that are below the $10k reporting threshold (e.g., between $7k and $10k)
- Cash involving multiple lower transactions (e.g., $3k) that over a period of time aggregate to a substantial sum
- Cash aggregated by tax identification number, customer information file number, or other identifier such as address or telephone number

Funds transfer records

Wire transfer reviews can also help the bank identify patterns of unusual activity. The frequency of these reviews will be determined by the bank's risk profile and the volume of activity and reports may focus on identifying higher-risk geographic locations and larger dollar funds transfer transactions.

When creating these reports, whether manually or using software, filters are set to identify transactions for review. For example, the report may identify groups of noncustomer transactions or payable upon proper identification (PUPID) transactions. Activities identified should be subjected to additional research to ensure the activity is consistent with stated account purpose and expected activity. When inconsistencies are identified, the institution may need to investigate further to determine if a SAR is warranted.
1. Identifying the Suspicious Activity

The level of review of any daily or monthly reports should be based on risk and should cover the bank’s higher-risk products, services, customers, entities, and geographic locations. The dollar threshold set for review is discretionary but should be set to allow the bank to detect unusual activity that is outside the norms set by the bank.

When unusual activity is identified, the bank’s BSA officer or risk officer will evaluate all relevant information to determine whether the activity is really suspicious.

Management should periodically evaluate the appropriateness of filtering criteria and thresholds. Each institution should evaluate and identify filtering criteria most appropriate for their institution. In addition, programming of institution’s monitoring systems should be independently reviewed and evaluated for reasonable filtering criteria.
1. Identifying the Suspicious Activity

Surveillance monitoring
Surveillance monitoring is an automated type of transaction monitoring which may combine multiple types of transactions and is likely to use various rules to identify individual transactions, patterns of activity, or deviations from expected activity. The programs may be off-the-shelf or developed and customized in-house, but they are designed to capture a wide range of account activity, such as cash activity, funds transfers, ACH, and ATM transactions, and include rule-based and intelligent systems to detect unusual or higher-risk transactions.

Surveillance monitoring is generally more sophisticated than transaction monitoring since transaction monitoring is only based on a single rule (e.g., transaction greater than $10,000). Surveillance monitoring, though, applies multiple overlapping rules, and filters or “alerts” that are more complex to identify potentially suspicious transactions.
1. Identifying the Suspicious Activity

The parameters and filters used in such system must be reasonable and tailored to activity that institution is trying to identify or control. When installing such a system, bank management will review the system prior to implementation to identify any gaps (common money laundering techniques or frauds) that may not have been addressed.

**Example**
The institution may have set their filters for cash structuring to only be triggered by a daily cash transaction aggregation in excess of $10,000 (CTR threshold). The bank may need to refine the filters to avoid missing potentially suspicious activity because common cash structuring techniques often involve transactions slightly under the CTR threshold or ones conducted over several days.

**Note:** When a bank uses an automated system, it will be asked to validate two elements. First, the bank must validate that the system itself is properly constructed and works in conjunction with the risk profile. Second, the bank will be expected to periodically check the filter settings to make sure they are working properly and capture the appropriate transactions for review and investigation.
1. Identifying the Suspicious Activity

Self Check Quiz

Which type of transaction monitoring report can help identify possible cash structuring through purchases of cashier’s checks, official bank checks, money orders, gift cards, or traveler’s checks?

» Select the correct answer and click Submit.

A) Currency activity reports
B) Funds transfer records
C) Monetary instrument records
D) Overdraft reports

C is correct.

A is incorrect because these reports are used to help the bank file Currency Transaction Reports and identify suspicious cash activity. B is incorrect because these reports are used to help the bank identify patterns of unusual activity. D is incorrect because Overdraft reports are not a type of transaction monitoring report.

Page 35
1. Identifying the Suspicious Activity

Question: Which type of monitoring system is generally more sophisticated—surveillance monitoring or transaction monitoring?

Answer: Surveillance monitoring is generally more sophisticated than transaction monitoring since transaction monitoring is only based on a single rule (e.g., transaction greater than $10,000). Surveillance monitoring, though, applies multiple, overlapping rules, and filters or “alerts” that are more complex to identify potentially suspicious transactions.
2. Managing Alerts

The second component in the process is a method for managing alerts so they do not become overwhelming. The bank must have systems in place to investigate alerts and be sure there are processes and staff assigned to evaluate any unusual activity, no matter how it has been identified.

Typically, in managing alerts, the bank will take the following steps:

- Have policies and procedures in place for referring unusual activity from all areas of the bank or business lines to the personnel responsible for evaluation and reporting
- Establish clear and defined escalation processes from the point of initial detection to conclusion of the investigation
- Assign adequate staff to identify, evaluate, and report potentially suspicious activities
2. Managing Alerts

The bank should assign adequate staff to the identification, evaluation, and reporting of potentially suspicious activities, taking into account the bank’s overall risk profile and the volume of transactions. Additionally, a bank should ensure that the assigned staff are experienced and provided with comprehensive and ongoing training to maintain their expertise. Staff should also be provided with sufficient internal and external tools to allow them to properly research activities and formulate conclusions.

After thorough research and analysis, investigators should document conclusions including any recommendation regarding whether or not to file a SAR. When multiple departments are responsible for researching unusual activities (for example, when the BSA department researches BSA-related activity and the Fraud department researches fraud-related activity), the lines of communication between the departments must remain open. This ensures that all suspicious activity is identified, evaluated, and reported.
2. Managing Alerts

Question:
What steps will banks typically take when managing alerts?

Answer:

- Have policies and procedures in place for referring unusual activity from all areas of the bank or business lines to the personnel responsible for evaluation and reporting
- Establish clear and defined escalation processes from the point of initial detection to conclusion of the investigation
- Assign adequate staff to identify, evaluate, and report potentially suspicious activities
3. Decision Making

The decision making part of the process is the final decision whether to report a transaction or activity by filing a SAR. After thorough research and analysis, all the findings are forwarded to the final decision maker, which may be an individual or a committee. Therefore, the bank should have policies and procedures for referring unusual activity from all business lines to personnel responsible. Those procedures should include a clear and defined escalation process from point of initial detection to conclusion of investigation that will explain what to do when an unusual transaction has been identified.

Decision makers should have the authority to make the final SAR filing decision. If the decisions are made by a committee, the committee should have a clearly defined process to resolve differences of opinion on filing decisions.

Decision making often requires inherently subjective judgment, so the decision maker(s) should document SAR decisions, including the specific reason for filing or not filing a SAR. This is especially important since the decision to file is based on a unique set of facts and circumstances and is a subjective decision.

Employees who refer possible suspicious activity to the bank officer designated to investigate such activity may never know if a SAR was filed, and that is how it should be. SAR filing is highly confidential and should not be discussed with any employee who does not have a “need to know.”

Because auditors and examiners will review individual decisions in connection with an evaluation of the process, the documentation of the decision will be important.
3. Decision Making

True or False?

Employees who refer possible suspicious activity to the bank officer designated to investigate such activity are notified within 30 days if a SAR is filed.

» Select the correct answer.

True
False

The statement is false because employees who refer possible suspicious activity to the bank officer designated to investigate such activity may never know if a SAR was filed. SAR filing is highly confidential and should not be discussed with any employee who does not have a “need to know.”
4. Completion and Filing

Completing the SAR

Although you may not be responsible for the actual completion of a SAR, the information you provide to the individual at your bank who does the filing is crucial. Remember that the law enforcement representatives who read the SAR will not be familiar with bank-specific product names or banking buzz-words. Make sure any novel or proprietary terms are described in detail so that they are understandable by “the man on the street.”

Banks should provide the most complete filing information available regardless of whether or not the individual fields are deemed critical for technical filing purposes.

All filings with FinCEN, including SARs, must be filed electronically with the Financial Crime Enforcement Network (FinCEN) BSA E-Filing System.

Although the basic information fields must be completed on a SAR, the SAR contains an area known as the “SAR Narrative.” This part of the SAR tells the story so that law enforcement can understand what led the bank to believe the activity was suspicious. Law enforcement agencies rely on this information to assist in money laundering, terrorist financing, and financial crimes investigations. The SAR Narrative should include enough information to explain clearly who was involved, what took place, when and where the activity happened, and why the bank believes the transaction was suspicious.

» Click the EZ Reference button to download and print a sample SAR.

Sidebar: Filers may attach a small file, and the contents of that file must be described in the SAR Narrative. Filers may not include any other supporting documentation with the FinCEN SAR. Instead, they should use the SAR Narrative to describe the other supporting documentation not included in the file. This supporting documentation, such as copies of instruments; receipts; sale, transaction or clearing records; photographs; and surveillance (audio or video recordings) must be made available to appropriate authorities upon request. Filers must retain all supporting documentation or a business record equivalent for five (5) years from the date of the report. Banks may also submit an Excel spreadsheet with detailed information about specific transactions and fund transfers or other analytics. The new addition also states these Excel spreadsheets are considered part of the narrative but do not take the place of the narrative (“narratives should not simply state ‘see attachment’”). Finally, the new provision affirms that, as part of the SAR filing, any supplemental material filed on an Excel spreadsheet with the SAR should be treated as confidential.
4. Completion and Filing

Any failure to adequately describe the factors that make the activity suspicious undermines the very purpose of the SAR and lessens its usefulness to law enforcement. The goal is to tell law enforcement what happened and why your bank thinks there is something suspicious about what took place.

» Roll over each button to see examples of questions to ask yourself when determining what information you need when reporting possible suspicious activity to the appropriate person at your bank.

- Who is conducting the activity? This includes names of businesses or individuals as well as other relevant facts about those individuals which all are important pieces of the information provided on a SAR. These may include the following:
  - Employer and occupation information
  - Relationship between the suspect and the filing institution
  - Length of the financial relationship between the subject and the bank

- What instruments or mechanisms were used or involved in the suspicious transactions? Examples include the following:
  - Fraudulent documents
  - Cash deposits/withdrawals
  - Wires or other electronic transactions
  - Stocks, bonds, or notes
  - Loans

- When did the activity take place? It helps to identify all accounts and transactions that were involved in chronological order by date and amount.

- Where did the suspicious activity take place? Identify the branch, department, or other locations where the activity occurred by name and street address.

- Why does the SAR filer think the activity is suspicious? Describe concisely but fully why your institution thinks the transactions are suspicious.

- How did the suspicious activity occur? Describe how the suspect transactions or pattern of transactions were completed. For account activity, provide as completely as possible an explanation of the cycle of funds including the source of the funds and the application of those funds.
Warning: Sometimes, it is important to alert law enforcement about a transaction or activity immediately, before a SAR is filed. If you think that may be necessary, your bank procedures will explain who to alert and how. It may be your immediate supervisor or it may be the bank’s BSA officer but the bank will have procedures in place on what steps to take.
4. Completion and Filing

Timeframe for filing a SAR

Once an activity has been determined to be suspicious, SAR regulations require the bank to file a SAR within 30 days. However, if no suspect has been identified, the window for filing a SAR expands to 60 days. What is important to understand, though, is that the clock does not start when a transaction is flagged. The time period for filing a SAR starts when an organization, during its review or because of other factors, knows or has reason to suspect that the activity or transaction under review meets one or more of the definitions of suspicious activity.

Banks must ensure that all SARs are completed accurately and properly filed within required timeframes. Prompt filing of SARs helps law enforcement identify and respond promptly to potential criminal activities. On the other hand, delayed filings are particularly detrimental when terrorist financing is suspected, in criminal cases where asset seizures are possible, or when significant fraud threatens the viability of a depository institution. This is why there may be times when law enforcement should be contacted directly.

The individual or individuals at your bank responsible for filing a SAR must follow the statutory SAR filing timeframes. Since alerting the person who will investigate and determine whether to file a SAR is the first step in the process, that timeframe may be significantly shorter than the statutory timeframe to let that person research and investigate the matter. You should consult your bank’s BSA policy to determine how to comply in order to meet the filing deadlines.

Corrected or amended reports

Sometimes, additional information will be discovered or an error identified in a SAR that has already been filed. If that does happen, it should be brought to the attention of the person at the bank who is responsible for filing SARs. If necessary, they will file a corrected or amended SAR in accordance with FinCEN procedures.

Note: In addition to filing the reports and forms in a timely manner, banks must retain all records pertaining to BSA reporting for a minimum of five years.
4. Completion and Filing

Requests by law enforcement to review documentation

Sometimes, law enforcement will want to review the documentation that forms the basis for filing the SAR, such as transaction records or account statements. SAR backup information and related information about the subject of the report can be given to an authorized law enforcement official, but there are procedures that most institutions will want to follow before helping the representative with their inquiry.

If you are approached by any law enforcement representatives requesting follow-up information about suspicious activity that the bank reported, you should refer the matter to your BSA officer for coordination. If a law enforcement agent asks you for information, explain that it is best handled by the appropriate officer at the bank since they have all the necessary information and can provide it in the right way.
4. Completion and Filing

Closing an account
A financial institution may use its reasonable business judgment to decide whether to close an account after a SAR filing has been made. It would be prudent for a bank to implement additional monitoring of an account that is the subject of a SAR filing, particularly if numerous SAR filings are involved. The ultimate decision to maintain or close an account will be made by each financial institution in accordance with its own standards and guidelines.

There are times, however, when a financial institution has an account with suspicious or potential criminal activity and law enforcement requests that the financial institution keep the account open. Financial institutions should ask for a written request from the law enforcement agency. This request should be issued by a supervisory agent or by an attorney within a United States Attorney’s Office or another office of the Department of Justice. If the request is made by a state or local law enforcement agency, the request should be from a supervisor of the state or local law enforcement agency or from an attorney within a state or local prosecutor’s office. The request should indicate that the agency requested that the financial institution maintain the account and the purpose of the request. The request should also indicate the duration of the request, not to exceed six months (law enforcement may issue a subsequent request for a longer duration).

Although the Bank Secrecy Act does not have a recordkeeping requirement with respect to these requests, FinCEN advises financial institutions to maintain the request for at least 5 years after the request has expired.
4. Completion and Filing

Self Check Quiz

In addition to filing the reports and forms in a timely manner, how long must banks retain records pertaining to BSA reporting?

» Select the correct answer and click Submit.

- A) Minimum of three years
- B) Minimum of five years
- C) Minimum of seven years
- D) Minimum of ten years

B is correct.
A, C, and D are incorrect because banks must retain all records pertaining to BSA reporting for a minimum of five years.
5. Monitoring and SAR Filing on Continuing Activity

SAR filing on continuing activity

Sometimes, an activity will continue after a SAR has been filed. If the activity continues, that should be brought to the attention of law enforcement. FinCEN guidelines suggest that activity should be reported on a regular basis, a process which also helps the bank monitor for potential problems. As a result, banks should have policies and procedures about when to escalate issues or problems identified as the result of repeat SAR filings on accounts.

These procedures should include the following elements:

- Review by senior management and legal staff (e.g., BSA compliance officer or SAR committee)
- Criteria for when analysis of the overall customer relationship is necessary
- Criteria for whether and, if so, when, to close the account
- Criteria for when to notify law enforcement

When filing SARs on continuing activity the generally accepted threshold is to review an activity 90 days after the most recent SAR with a goal for filing the next SAR 120 days after the most recently filed SAR.

Identifying the suspicious activity

Managing alerts

Decision making

Completion and filing

Monitoring and SAR Filing on Continuing Activity

When filing an ongoing SAR, they would like to see the full scope of the activity. For instance, say that you are filing a report on the activity from March 22 through June 22, 2016. Those are the dates that you would enter on the SAR that you are filing. HOWEVER, if the original SAR was prompted by something that occurred in December 2015, that should be noted in the narrative along with something to connect this SAR with the prior SARs. That makes law enforcement’s task easier.
5. Monitoring and SAR Filing on Continuing Activity

SAR filing on continuing activity
What is most helpful for law enforcement is to report the range of activity that you have reviewed. When you file an ongoing SAR, they would like two specific bits of information (that way they know what’s been covered). In Field 27 of the SAR, what they would like are the dates for the review for that particular SAR. In other words, you would enter the full 90-day range of activity that you have reviewed. Meanwhile, in the SAR, what they would also like to see is information about the full scope of the activity. For instance, say that you are filing a report on the activity from March 22 through June 22, 2018. Those are the dates that you would enter on the SAR that you are filing. HOWEVER, if the original SAR was prompted by something that occurred in December 2017, that should be noted in the narrative along with something to connect this SAR with the prior SARs. That makes law enforcement’s task easier.
5. Monitoring and SAR Filing on Continuing Activity

Marijuana related businesses and SAR filing

Even though many states have taken steps to decriminalize the use of marijuana, for both medicinal purposes and recreational use, federal law still makes the possession and distribution of marijuana illegal. The Controlled Substances Act classifies marijuana as a Schedule 1 drug, similar to heroin and LSD. Therefore, under federal law, processing funds connected with a marijuana business is technically money laundering.

The Department of Justice has issued guidance that indicates that activities in compliance with state law may not be prosecuted and FinCEN has issued guidance for reporting suspicious activities but offering banking services to a marijuana-related business carries a level of risk that should only be undertaken after careful consultation with bank counsel.

Page 50
5. Monitoring and SAR Filing on Continuing Activity

Question: When filing SARs on continuing activity, what is the threshold for reviewing the subject activity?

Answer. The generally accepted threshold is to review an activity 90 days after the most recent SAR with a goal for filing the next SAR 120 days after the most recently filed SAR.
Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States’ ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Examiners and banks should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system.

Knowing all of the controls, due diligence techniques, and red flags is not necessarily enough to ensure that an institution is effectively monitoring for and reporting on suspicious activity. A control breakdown commonly noted by examiners is ineffective or inefficient reporting of suspicious activity by bank personnel. Not only should all staff be educated about what to look for, but they should be equally educated on how to report suspicious activity within the institution. This helps to ensure a seamless process that will eventually result in either documentation of rationale supporting why certain activities are not suspicious or the filing of a SAR.

By completing BSA/AML: SAR Filing, you learned about the scope of activities appropriate for SAR filing and the importance of keeping SARs confidential. You also learned about indicators of suspicious activity, the five key components of SAR filing, and marijuana related businesses and SAR filing.

» Click Exit to close this course.