Suspicious Activity Reporting — Overview

Objective. *Assess the bank's policies, procedures, and processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities.*

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.

Within this system, FinCEN and the federal banking agencies recognize that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through the bank. Examiners should focus on evaluating a bank's policies, procedures, and processes to identify, evaluate, and report suspicious activity. However, as part of the examination process, examiners should review individual SAR filing decisions to determine the effectiveness of the bank's suspicious activity identification, evaluation, and reporting process. Banks, bank holding companies, and their subsidiaries are required by federal regulations[53] to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
  - May involve potential money laundering or other illegal activity (e.g., terrorism financing).[54]
  - Is designed to evade the BSA or its implementing regulations.[55]
  - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit,

[53] Refer to 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Board of Governors of the Federal Reserve System) (Federal Reserve); 12 CFR 353 (Federal Deposit Insurance Corporation)(FDIC); 12 CFR 748 (National Credit Union Administration)(NCUA); 12 CFR 21.11 and 12 CFR 163.180 (Office of the Comptroller of the Currency)(OCC); and 31 CFR 1020.320 (FinCEN).

[54] FinCEN issued guidance identifying certain BSA expectations for banks offering services to marijuana-related businesses, including expectations for filing SARs, FIN-2014-G001, February 14, 2014.

[55] Refer to Appendix G ("Structuring") for additional guidance.

or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

Safe Harbor for Banks From Civil Liability for Suspicious Activity Reporting

Federal law (31 USC 5318(g)(3)) provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. Specifically, the law provides that a bank and its directors, officers, employees, and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.[56]

Systems to Identify, Research, and Report Suspicious Activity

Suspicious activity monitoring and reporting are critical internal controls. Proper monitoring and reporting processes are essential to ensuring that the bank has an adequate and effective BSA compliance program. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The sophistication of monitoring systems should be dictated by the bank's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies. The bank should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking 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.

Generally, effective suspicious activity monitoring and reporting systems include five key components (refer to Appendix S "Key Suspicious Activity Monitoring Components"). The 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. The five key components to an effective monitoring and reporting system are:

[56] The agencies incorporated the statutory expansion of the safe harbor by cross-referencing section 5318(g) in their SAR regulations. The OCC and FinCEN amended their SAR regulations to make clear that the safe harbor also applies to a disclosure by a bank made jointly with another financial institution for purposes of filing a joint SAR (see 12 CFR 21.11(l) and 31 CFR 1020.320(e)), respectively.

- Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output).
- Managing alerts.
- SAR decision making.
- SAR completion and filing.
- Monitoring and SAR filing on continuing activity.

These components are present in banks of all sizes. However, the structure and formality of the components may vary. Larger banks typically have greater differentiation and distinction between functions, and may devote entire departments to the completion of each component. Smaller banks may use one or more employees to complete several tasks (e.g., review of monitoring reports, research activity, and completion of the actual SAR). Policies, procedures, and processes should describe the steps the bank takes to address each component and indicate the person(s) or departments responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file, SAR completion and filing, and monitoring and SAR filing on continuing activity.

Identification of Unusual Activity

Banks use a number of methods to identify potentially suspicious activity, including but not limited to activity identified by employees during day-to-day operations, law enforcement inquiries, or requests, such as those typically seen in section 314(a) and section 314(b) requests, advisories issued by regulatory or law enforcement agencies, transaction and surveillance monitoring system output, or any combination of these.

Employee Identification

During the course of day-to-day operations, employees may observe unusual or potentially suspicious transaction activity. Banks should implement appropriate training, policies, and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity. Banks should be aware of all methods of identification and should ensure that their suspicious activity monitoring system includes processes to facilitate the transfer of internal referrals to appropriate personnel for further research.

Law Enforcement Inquiries and Requests

Banks should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects when appropriate, identifying unusual or potentially suspicious activity related to those subjects, and filing, as appropriate, SARs related to those subjects. Law enforcement inquiries and requests can include grand jury subpoenas, National Security Letters (NSL), and section 314(a) requests.[57]

[57] Refer to core overview section, "Information Sharing," page 92, for a discussion on section 314(a) requests.

Mere receipt of any law enforcement inquiry does not, by itself, require the filing of a SAR by the bank. Nonetheless, a law enforcement inquiry may be relevant to a bank's overall risk assessment of its customers and accounts. For example, the receipt of a grand jury subpoena should cause a bank to review account activity for the relevant customer.[58] A bank should assess all of the information it knows about its customer, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program.

The bank should determine whether a SAR should be filed based on all customer information available. Due to the confidentiality of grand jury proceedings, if a bank files a SAR after receiving a grand jury subpoena, law enforcement discourages banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Rather, the SAR should reference only those facts and activities that support a finding of suspicious transactions identified by the bank.

National Security Letters

NSLs are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following:

- Telephone and electronic communications records from telephone companies and Internet service providers.[59]
- Information from credit bureaus.[60]
- Financial records from financial institutions.[61]

NSLs are highly confidential documents; for that reason, examiners do not review or sample specific NSLs.[62] Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. Banks that receive NSLs must take appropriate measures to ensure the confidentiality of the letters and should have procedures in place for processing and maintaining the confidentiality of NSLs.

If a bank files a SAR after receiving a NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the bank.

Questions regarding NSLs should be directed to the bank's local FBI field office. Contact information for the field offices can be found at www.fbi.gov.

---

[58] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance" *The SAR Activity Review – Trends, Tips & Issues*, Issue 10, May 2006, pages 42 – 44, on the FinCEN Web site.

[59] Electronic Communications Privacy Act, 18 USC 2709.

[60] Fair Credit Reporting Act, 15 USC 1681u.

[61] Right to Financial Privacy Act of 1978, 12 USC 3401 *et seq.*

[62] Refer to the Bank Secrecy Act Advisory Group, *The SAR Activity Review — Trends, Tips & Issues*, Issue 8, April 2005 for further information on NSLs which is available on the FinCEN Web site.

Transaction Monitoring (Manual Transaction Monitoring)

A transaction monitoring system, sometimes referred to as a manual transaction monitoring system, typically targets specific types of transactions (e.g., those involving large amounts of cash, those to or from foreign geographies) and includes a manual review of various reports generated by the bank's MIS or vendor systems in order to identify unusual activity. Examples of MIS reports include currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, ATM transaction reports, and nonsufficient funds (NSF) reports. Many MIS or vendor systems include filtering models for identification of potentially unusual activity. The process may involve review of daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the bank's BSA/AML risk profile and appropriately cover its higher-risk products, services, customers, entities, and geographic locations.

MIS or vendor system-generated reports typically use a discretionary dollar threshold. Thresholds selected by management for the production of transaction reports should enable management to detect unusual activity. Upon identification of unusual activity, assigned personnel should review CDD and other pertinent information to determine whether the activity is suspicious. Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. Each bank should evaluate and identify filtering criteria most appropriate for their bank. The programming of the bank's monitoring systems should be independently reviewed for reasonable filtering criteria. Typical transaction monitoring reports are as follows.

Currency activity reports. Most vendors offer reports that identify all currency activity or currency activity greater than $10,000. These reports assist bankers with filing CTRs and identifying suspicious currency activity. Most bank information service providers offer currency activity reports that can filter transactions using various parameters, for example:

- Currency activity including multiple transactions greater than $10,000.
- Currency activity (single and multiple transactions) below the $10,000 reporting requirement (e.g., between $7,000 and $10,000).
- Currency transactions involving multiple lower dollar transactions (e.g., $3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g., $30,000).
- Currency transactions aggregated by customer name, taxpayer identification number, or customer information file number.

Such filtering reports, whether implemented through a purchased vendor software system or through requests from information service providers, significantly enhance a bank's ability to identify and evaluate unusual currency transactions.

Funds transfer records. The BSA requires banks to maintain records of funds transfer in amounts of $3,000 and above. Periodic review of this information can assist banks in identifying patterns of unusual activity. A periodic review of the funds transfer records in banks with low funds transfer activity is usually sufficient to identify unusual activity. For

banks with more significant funds transfer activity, use of spreadsheet or vendor software is an efficient way to review funds transfer activity for unusual patterns. Most vendor software systems include standard suspicious activity filter reports. These reports typically focus on identifying certain higher-risk geographic locations and larger dollar funds transfer transactions for individuals and businesses. Each bank should establish its own filtering criteria for both individuals and businesses. Noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions should be reviewed for unusual activity. Activities identified during these reviews should be subjected to additional research to ensure that identified activity is consistent with the stated account purpose and expected activity. When inconsistencies are identified, banks may need to conduct a global relationship review to determine if a SAR is warranted.

Monetary instrument records. Records for monetary instrument sales are required by the BSA. Such records can assist the bank in identifying possible currency structuring through the purchase of cashier's checks, official bank checks, money orders, or traveler's checks in amounts of $3,000 to $10,000. A periodic review of these records can also help identify frequent purchasers of monetary instruments and common payees. Reviews for suspicious activity should encompass activity for an extended period of time (30, 60, 90 days) and should focus on, among other things, identification of commonalities, such as common payees and purchasers, or consecutively numbered purchased monetary instruments.

Surveillance Monitoring (Automated Account Monitoring)

A surveillance monitoring system, sometimes referred to as an automated account monitoring system, can cover multiple types of transactions and use various rules to identify potentially suspicious activity. In addition, many can adapt over time based on historical activity, trends, or internal peer comparison. These systems typically use computer programs, developed in-house or purchased from vendors, to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from the bank's core data processing system. Banks that are large, operate in many locations, or have a large volume of higher-risk customers typically use surveillance monitoring systems.

Surveillance monitoring systems include rule-based and intelligent systems. Rule-based systems detect unusual transactions that are outside of system-developed or management-established "rules." Such systems can consist of few or many rules, depending on the complexity of the in-house or vendor product. These rules are applied using a series of transaction filters or a rules engine. Rule-based systems are more sophisticated than the basic manual system, which only filters on one rule (e.g., transaction greater than $10,000). Rule-based systems can apply multiple rules, overlapping rules, and filters that are more complex. For example, rule-based systems can initially apply a rule, or set of criteria to all accounts within a bank (e.g., all retail customers), and then apply a more refined set of criteria to a subset of accounts or risk category of accounts (e.g., all retail customers with direct deposits). Rule-based systems can also filter against individual customer-account profiles.

Intelligent systems are adaptive and can filter transactions, based on historical account activity or compare customer activity against a pre-established peer group or other relevant data. Intelligent systems review transactions in context with other transactions and the customer profile. In doing so, these systems increase their information database on the customer, account type, category, or business, as more transactions and data are stored in the system.

Relative to surveillance monitoring, system capabilities and thresholds refer to the parameters or filters used by banks in their monitoring processes. Parameters and filters should be reasonable and tailored to the activity that the bank is trying to identify or control. After parameters and filters have been developed, they should be reviewed before implementation to identify any gaps (common money laundering techniques or frauds) that may not have been addressed. For example, a bank may discover that its filter for cash structuring is triggered only by a daily cash transaction in excess of $10,000. The bank may need to refine this filter in order to avoid missing potentially suspicious activity because common cash structuring techniques often involve transactions that are slightly under the CTR threshold.

Once established, the bank should review and test system capabilities and thresholds on a periodic basis. This review should focus on specific parameters or filters in order to ensure that intended information is accurately captured and that the parameter or filter is appropriate for the bank's particular risk profile.

Understanding the filtering criteria of a surveillance monitoring system is critical to assessing the effectiveness of the system. System filtering criteria should be developed through a review of specific higher-risk products and services, customers and entities, and geographies. System filtering criteria, including specific profiles and rules, should be based on what is reasonable and expected for each type of account. Monitoring accounts purely based on historical activity can be misleading if the activity is not actually consistent with similar types of accounts. For example, an account may have a historical transaction activity that is substantially different from what would normally be expected from that type of account (e.g., a check-cashing business that deposits large sums of currency versus withdrawing currency to fund the cashing of checks).

The authority to establish or change expected activity profiles should be clearly defined through policies and procedures. Controls should ensure limited access to the monitoring systems, and changes should generally require the approval of the BSA compliance officer or senior management. Management should document and be able to explain filtering criteria, thresholds used, and how both are appropriate for the bank's risks. Management should also periodically review and test the filtering criteria and thresholds established to ensure that they are still effective. In addition, the monitoring system's programming methodology and effectiveness should be independently validated to ensure that the models are detecting potentially suspicious activity. The independent validation should also verify the policies in place and that management is complying with those policies.

Managing Alerts

Alert management focuses on processes used to investigate and evaluate identified unusual activity. Banks should be aware of all methods of identification and should ensure that their suspicious activity monitoring program includes processes to evaluate any unusual activity identified, regardless of the method of identification. Banks should have policies, procedures, and processes in place for referring unusual activity from all areas of the bank or business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

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 possess the requisite experience levels and are 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.

Internal research tools include, but are not limited to, access to account systems and account information, including CDD and EDD information. CDD and EDD information assist banks in evaluating if the unusual activity is considered suspicious. For additional information, refer to the core overview section, "Customer Due Diligence," page 56. External research tools may include widely available Internet media search tools, as well those accessible by subscription. 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 (i.e., 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 allows banks with bifurcated processes to gain efficiencies by sharing information, reducing redundancies, and ensuring all suspicious activity is identified, evaluated, and reported.

If applicable, reviewing and understanding suspicious activity monitoring across the organizations' affiliates, subsidiaries, and business lines may enhance a banking organization's ability to detect suspicious activity, and thus minimize the potential for financial losses, increased legal or compliance expenses, and reputational risk to the organization. Refer to the expanded overview section, "BSA/AML Compliance Program Structures," page 155, for further guidance.

Identifying Underlying Crime

Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing,[63] and certain other crimes above prescribed dollar thresholds.

[63] If a bank knows, suspects, or has reason to suspect that a customer may be linked to terrorist activity against the United States, the bank should immediately call FinCEN's Financial Institutions terrorist hot line toll-free number (866) 556-3974. Similarly, if any other suspected violation — such as an ongoing money laundering

However, banks are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). Investigation is the responsibility of law enforcement. When evaluating suspicious activity and completing the SAR, banks should, to the best of their ability, identify the characteristics of the suspicious activity. Suspicious Activity Information, Part II of the SAR provides a number of categories with different types of suspicious activity. Within each category, there is the option of selecting "Other" if none of the suspicious activities apply. However, the use of "Other" should be limited to situations that cannot be broadly identified within the categories provided.

SAR Decision Making

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker (individual or committee). The bank should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The decision maker, whether an individual or committee, should have the authority to make the final SAR filing decision. When the bank uses a committee, there should be a clearly defined process to resolve differences of opinion on filing decisions. Banks should document SAR decisions, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. However, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact that each suspicious activity reporting decision is based on unique facts and circumstances, no single form of documentation is required when a bank decides not to file.[64]

The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the bank has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.[65]

SAR Filing on Continuing Activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is

scheme — requires immediate attention, the bank should notify the appropriate federal banking and law enforcement agencies. In either case, the bank must also file a SAR.

[64] Bank Secrecy Act Advisory Group, "Section 4 — Tips on SAR Form Preparation & Filing," *The SAR Activity Review — Trends, Tips & Issues*, Issue 10, May 2006, page 38, on the FinCEN Web site.

[65] Refer to Appendix R ("Interagency Enforcement Statement") for additional information.

accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement and the federal banking agencies. FinCEN's guidelines have suggested that banks should report continuing suspicious activity by filing a report at least every 90 calendar days. Subsequent guidance permits banks with SAR requirements to file SARs for continuing activity after a 90 day review with the filing deadline being 120 calendar days after the date of the previously related SAR filing. Banks may also file SARs on continuing activity earlier than the 120-day deadline if the bank believes the activity warrants earlier review by law enforcement.[66] This practice notifies law enforcement of the continuing nature of the activity in aggregate. In addition, this practice reminds the bank that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as bank management determining that it is necessary to terminate a relationship with the customer or employee that is the subject of the filing.

Banks should be aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that a bank maintain a particular account, the bank should ask for a written request. The written request should indicate that the agency has requested that the bank maintain the account and the purpose and duration of the request. Ultimately, the decision to maintain or close an account should be made by a bank in accordance with its own standards and guidelines.[67]

The bank should develop policies, procedures, and processes indicating when to escalate issues or problems identified as the result of repeat SAR filings on accounts. The procedures should include:

- 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, if appropriate.

SAR Completion and Filing

SAR completion and filing are a critical part of the SAR monitoring and reporting process. Appropriate policies, procedures, and processes should be in place to ensure SARs are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing. FinCEN developed a new electronic BSA Suspicious Activity Report (BSAR) that replaced FinCEN SAR-DI form TD F 90-22.47. The BSAR provides a uniform data collection format that can be used across multiple industries. As of April 1, 2013, the BSAR is mandatory and must be filed through

[66] Refer to Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report, Question #16.

[67] Refer to *Requests by Law Enforcement for Financial Institutions to Maintain Accounts*, June 13, 2007.

FinCEN's BSA E-Filing System. The BSAR does not create or otherwise change existing statutory and regulatory expectations for banks.

The BSAR includes a number of additional data elements pertaining to the type of suspicious activity and the financial services involved. Certain fields in the BSAR are marked as "critical" for technical filing purposes. This means the BSA E-Filing System does not accept filings in which these fields are left blank. For these items, the bank must either provide the requested information or check the "unknown" box that is provided with each critical field. Banks should provide the most complete filing information available consistent with existing regulatory expectations, regardless of whether or not the individual fields are deemed critical for technical filing purposes.[68]

Banks should report the information that they know, or that otherwise arises, as part of their case reviews. Other than the critical fields, the addition of the new and expanded data elements does not create an expectation that banks will revise internal programs, or develop new programs, to capture information that reflects the expanded lists.[69] Refer to Appendix T for additional information on filing through the BSA E-Filing System.

Timing of a SAR Filing

The SAR rules require that a SAR be electronically filed through the BSA E-Filing System no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.[70]

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The bank's automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a

[68] Refer to *Filing FinCEN's new Currency Transaction Report and Suspicious Activity Report*, FIN-2012-G002, March 29, 2012.

[69] *Id*.

[70] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 1, October 2000, page 27.

determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulation.[71]

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time. What constitutes a "reasonable period of time" varies according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process of each bank. The key factor is that a bank has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.[72]

For situations requiring immediate attention, in addition to filing a timely SAR, a bank must immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the bank's primary regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a bank of its obligation to file a SAR.[73]

SAR Quality

Banks are required to file SARs that are complete, thorough, and timely. Banks should include all known subject information on the SAR. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. However, there may be legitimate reasons why certain information may not be provided in a SAR, such as when the filer does not have the information. A thorough and complete narrative may make the difference in determining whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Because the SAR narrative section is the only area summarizing suspicious activity, the section, as stated on the SAR, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

To inform and assist banks in reporting instances of suspected money laundering, terrorist financing, and fraud, FinCEN issues advisories and guidance containing examples of "red flags." In order to assist law enforcement in its efforts to target these activities, FinCEN requests that banks check the appropriate box(es) in the Suspicious Activity Information

[71] Bank Secrecy Act Advisory Group, "Section 5 — Issues and Guidance," *The SAR Activity Review — Trends, Tips & Issues*, Issue 10, May 2006, page 44. For examples of when the date of initial detection occurs, refer to *SAR Activity Review — Trends, Tips, and Issues*, Issue 14, October 2008, page 38.

[72] *Id*.

[73] For suspicious activity related to terrorist activity, institutions may also call FinCEN's Financial Institution's terrorist hot line's toll-free number (866) 556-3974 (seven days a week, 24 hours a day) to further facilitate the immediate transmittal of relevant information to the appropriate authorities.

section and include certain key terms in the narrative section of the SAR. The advisories and guidance can be found on FinCEN Web site.[74]

By their nature, SAR narratives are subjective, and examiners generally should not criticize the bank's interpretation of the facts. Nevertheless, banks should ensure that SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and are included within the SAR. The BSAR accepts a single, Microsoft Excel-compatible comma separated value (csv) file no larger than one (1) megabyte as an attachment as part of the report. This capability allows a bank to include transactional data such as specific financial transactions and funds transfers or other analytics that are more readable or usable in this format than it would be if otherwise included in the narrative. Such an attachment is be considered a part of the narrative and is not considered to be a substitute for the narrative. For example, narratives should not simply state "see attachment" if the bank included a csv attachment. As with other information that may be prepared in connection with the filing of a SAR, an attachment is considered supporting documentation and should be treated as confidential to the extent that it indicates the existence of a SAR.

More specific guidance is available in Appendix L ("SAR Quality Guidance") to assist banks in writing, and assist examiners in evaluating, SAR narratives.[75]

Notifying Board of Directors of SAR Filings

Banks are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and banks should have flexibility in structuring their format. Therefore, banks may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, banks may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the bank, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties, while being mindful of the confidential nature of the SAR.[76]

[74] For more information, refer to SAR Advisory Key Terms on the FinCEN Web site.

[75] Guidance to assist banks in filing SARs can be found in the *FinCEN Suspicious Activity Report (FinCEN SAR) Electronic Filing Requirements* Release Date October 2012, Version 1.2. Other guidance available from FinCEN includes "*Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting*" (October 10, 2007).

[76] As noted in the Bank Secrecy Act Advisory Group's *The SAR Activity Review — Trends, Tips & Issues*, Issue 2, June 2001, "In the rare instance when suspicious activity is related to an individual in the organization, such as the president or one of the members of the board of directors, the established policy that would require notification of a SAR filing to such an individual should not be followed. Deviations to established policies and procedures so as to avoid notification of a SAR filing to a subject of the SAR should be documented and appropriate uninvolved senior organizational personnel should be so advised."

Record Retention and Supporting Documentation

Banks must retain copies of SARs and supporting documentation for five years from the date of filing the SAR. The bank can retain copies in paper or electronic format. Additionally, banks must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or federal banking agency. "Supporting documentation" refers to all documents or records that assisted a bank in making the determination that certain activity required a SAR filing. No legal process is required for disclosure of supporting documentation to FinCEN or an appropriate law enforcement or federal banking agency.[77]

Prohibition of SAR Disclosure

No bank, and no 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. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR. [78] Furthermore, FinCEN and the federal banking agencies take the position that a bank's internal controls for the filing of SARs should minimize the risks of disclosure.

A bank or its agent may reveal the existence of a SAR to fulfill responsibilities consistent with the BSA, provided no person involved in a suspicious transaction is notified that the transaction has been reported. 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 to the full extent authorized in 31 USC 5318(g)(2)(B). 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.

Any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement[79] or federal banking agency, shall decline to produce the SAR or to provide

[77] Refer to *Suspicious Activity Report Supporting Documentation*, June 13, 2007.

[78] FinCEN and the OCC issued final rules amending the confidentiality provisions of suspicious activity reports. The rules clarify how, when, and to whom SAR information, and the existence of a SAR may be disclosed. Refer to 75 Fed. Reg. 75576 (December 3, 2010) (OCC) and 75 Fed. Reg. R 75593 (December 3, 2010) (FinCEN).

[79] Examples of agencies to which a SAR or the information contained therein could be provided include: the criminal investigative services of the armed forces; the Bureau of Alcohol, Tobacco, and Firearms; an attorney general, district attorney, or state's attorney at the state or local level; the Drug Enforcement Administration; the Federal Bureau of Investigation; the Internal Revenue Service or tax enforcement agencies at the state level; the Office of Foreign Assets Control; a state or local police department; a United States Attorney's Office; Immigration and Customs Enforcement; the U.S. Postal Inspection Service; and the U.S. Secret Service. For additional information, refer to Bank Secrecy Act Advisory Group, "Section 5—Issues and Guidance," *The SAR Activity Review—Trends, Tips & Issues,* Issue 9, October 2005, page 44 on the FinCEN Web site.

any information that would disclose that a SAR has been prepared or filed, citing 31 CFR 1020.320(e) and 31 USC 5318(g)(2)(A)(i). FinCEN and the bank's federal banking agency should be notified of any such request and of the bank's response.

Examiners should follow their respective agency's protocol on discovery of the improper disclosure of a SAR. Examiners also should ensure the bank has notified the appropriate federal banking agency and FinCEN of the improper disclosure.

Sharing SARs With Head Offices, Controlling Companies, and Certain U.S. Affiliates

Previously issued guidance clarified that sharing of a SAR or, more broadly, any information that would reveal the existence of a SAR, with a head office or controlling company (including overseas) 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. [80]

A controlling company as defined in the guidance includes:

- A bank holding company (BHC), as defined in section 2 of the BHC Act.
- A savings and loan holding company, as defined in section 10(a) of the Home Owners' Loan Act.
- A company having the power, directly or indirectly, to direct the management policies of an industrial loan company or a parent company or to vote 25 percent or more of any class of voting shares of an industrial loan company or parent company.

The guidance confirms that:

- A U.S. branch or agency of a foreign bank may share a SAR with its head office outside the United States.
- A U.S. bank may share a SAR with controlling companies whether domestic or foreign.

In addition, a bank that has filed a SAR may share the SAR, or any information that would reveal the existence of the SAR, with an affiliate provided the affiliate is subject to a SAR regulation.[81] An affiliate is defined as any company under common control with, or controlled by, that depository institution. 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

[80] *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies*, issued by FinCEN, Federal Reserve, FDIC, OCC, and OTS, January 20, 2006.

[81] *Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates*, issued by FinCEN, FIN-2010-G006, November 23, 2010.

- Controls in any manner the election of a majority of the directors or trustees of the company and the depository institution.

Controlled by means that the depository institution:

- Directly or indirectly has the power to vote 25 percent or more of any class of the voting securities of the company; or

- Controls in any manner the election of a majority of the directors or trustees of the company. See 12 USC 1841(a)(2).

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.