Four Key Components of a Suspicious Activity Monitoring Program
APPENDIX S: KEY SUSPICIOUS ACTIVITY MONITORING COMPONENTS

Identification of Unusual Activity
(Employee identification, law enforcement inquiries, other referrals, transaction, and surveillance monitoring systems)

Alert Management

SAR Decision Making

SAR Completion and Filing
IDENTIFICATION OF SUSPICIOUS ACTIVITY
Unusual Activity Identification

- Employee Identification
- Law Enforcement Requests
- National Security Letters
- Transaction Monitoring
- Surveillance Monitoring
Employee Identification
Employee Identification

• Activity identified by employees during day-to-day operations

• Critical to train staff
Employee Identification

- Employees need method to report suspicious activity to appropriate personnel
- Worksheet, e-mail, phone
- Central point of contact
- Documentation
- Lack of training?
# Sample Worksheet

## Suspicious Activity Worksheet

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Name:</td>
<td>Branch Reporting activity:</td>
</tr>
<tr>
<td>Account Number:</td>
<td>Employee Reporting:</td>
</tr>
<tr>
<td>Amount of suspicious activity: $</td>
<td>Contact phone:</td>
</tr>
<tr>
<td>Type of suspicious activity:</td>
<td>Contact email:</td>
</tr>
<tr>
<td>Describe why this activity is suspicious:</td>
<td></td>
</tr>
</tbody>
</table>

**Received by:**

**Date Received:**

**Other investigation comments:**

**Date investigation closed:**
Law Enforcement Inquiries and Requests
IDENTIFICATION

Law Enforcement Inquiries and Requests

- Include grand jury subpoenas, National Security Letters (NSL), and 314(a) requests
- Establish policies and procedures for
  - Identifying the subject of the request
  - Monitoring their transaction activity if appropriate
  - Identifying potentially suspicious activity and as appropriate when to file a SAR
Law Enforcement Inquiries and Requests

• Request does not, by itself, require the filing of a SAR

• But may be relevant to overall risk assessment of customer and their accounts
Law Enforcement Inquiries and Requests

• For example, receipt of a grand jury subpoena should cause a bank to review the account activity

• Then consider all you know about the customer, including the receipt of the inquiry when making a determination of risk

• Make the decision to file a SAR based on all information available
Law Enforcement Inquiries and Requests

PLEASE NOTE:

• Due to the confidentiality of grand jury proceedings, if institution files a SAR after receiving a grand jury subpoena, law enforcement **discourages financial institutions from including any reference to the receipt or existence of grand jury subpoena in the SAR**.

• Rather, the SAR should reference only the facts and circumstances that supported the finding of suspicious activity.
IDENTIFICATION

National Security Letters
National Security Letters (NSLs)

Written investigative demands

Issued by local FBI and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain:

- Telephone and electronic communications records from telephone companies and Internet service providers
- Information from credit bureaus
- Financial records from financial institutions
IDENTIFICATION

National Security Letters (NSLs)

- Highly confidential, even examiners will not review or sample specific NSLs
- 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
- Take appropriate measures to ensure confidentiality
- Have written policies and procedures in place for processing and maintaining confidentiality
IDENTIFICATION

National Security Letters (NSLs)

• If SAR is filed, it should not contain any reference to receipt or existence of NSL.

• Should only reference the facts and activities that supported decision to file a SAR.

• Direct questions on NSLs to the local FBI field office. Contact information for the FBI field offices can be found at www.fbi.gov.
Transaction Monitoring
Transaction Monitoring:
Also called Manual Transaction Monitoring system

- Targets specific types of transactions
- Manual review of various individual reports generated by institution’s host or other systems to identify unusual activity

For Example:
- Cash, Wire, or Monetary Instrument Sales Reports
- Significant Balance Change Reports
- Nonsufficient Funds (NSF) reports
- Structured Transaction Reports
Transaction Monitoring:

• Review of daily or monthly reports
• Type and frequency should be risk based and cover institution’s higher-risk products, services, customers, entities, and geographic locations
• Use a discretionary dollar threshold
• Thresholds selected should enable you to detect unusual activity
• After review, if unusual activity is identified, evaluate all relevant information to determine whether the activity is really suspicious
Transactions Monitoring:
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.

“Is your program sufficient for the risk level of your institution?”
Transaction Monitoring: Cash Reviews

- Assist with filing Currency Transaction Reports and identifying suspicious cash activity
- FFIEC Suggestions:
  - Cash aggregating 10K or more
  - Cash (single and multiple transactions) 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 of money (e.g., $30k)
  - Cash aggregated by tax identification number or customer information file number
TRANSACTION MONITORING

Transaction Monitoring: Funds Transfers

• Review for patterns of unusual activity
  – Periodic review for institutions with low activity is usually sufficient to identify anything unusual
  – For more significant activity, spreadsheets or software is needed to identify unusual patterns

• Reports may focus on identifying higher-risk geographic locations and larger dollar funds transfer transactions
Transaction Monitoring: Funds Transfers

- Establish filtering criteria for both individuals and businesses.
- Review noncustomer transactions and payable upon proper identification (PUPID) transactions.
- Activities identified should be subjected to additional research to ensure that activity is consistent with stated account purpose and expected activity.
- When inconsistencies are identified, the institution may need to conduct a global relationship review to determine if a SAR is warranted.
Transaction Monitoring: Monetary Instruments

- Records are required by the BSA
- Assist in identifying possible cash structuring when purchasing cashier’s checks, official bank checks, money orders, gift cards, or traveler’s checks
- Reviews for suspicious activity should encompass activity for an extended period of time (30, 60, 90 days) to assist in locating patterns such as:
  - Common payees
  - Common purchasers
  - Consecutively numbered monetary instruments
Surveillance Monitoring
Surveillance Monitoring:
Also called Automated Account Monitoring System
• Combines multiple types of transactions
• Use various rules
• Identify individual transactions, patterns of activity, or deviations from expected activity
• Can capture a wide range of account activity, such as cash activity, funds transfers, ACH, and ATM transactions and monetary instruments
• May include rule-based and intelligent systems to detect unusual or higher-risk transactions
Surveillance Monitoring:

- More sophisticated than transaction monitoring, which only filters on one rule (e.g., transaction greater than $10,000)
- May apply multiple rules, overlapping rules, and filters or “alerts” that are more complex
- May include adaptive-filter transactions, based on historical account activity (for example, spikes from average activity)
Surveillance Monitoring:

- Capabilities and thresholds refer to the parameters or alert filters used in the monitoring process.
- Parameters and filters:
  - Reasonable and tailored to activity that institution is trying to identify or control.
  - Should be reviewed before implementation to identify any gaps (common money laundering techniques or frauds) that may not have been addressed.
Surveillance Monitoring:

Example: 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)

• May need to refine filter to avoid missing potentially suspicious activity because common cash structuring techniques often involve
  – transactions slightly under the CTR threshold or
  – are conducted over several days
Surveillance Monitoring:

- Review and test system capabilities and thresholds on a periodic basis
- Focus on specific parameters or filters to ensure that suspicious or unusual activity will be captured
- Are the parameters or filters appropriate for institution’s particular risk profile
- Understanding the filters in your system and how your system works is critical to assessing the effectiveness of your monitoring program
Surveillance Monitoring:

- When developing filters, consider institution’s higher-risk products & services, customers & entities, & geographies
- Filters should be based on what is reasonable & expected for each type of account
Surveillance Monitoring:

- Monitoring based solely on historical activity can be misleading if the activity is not consistent with similar types of accounts & customers

- Account may have historical activity that is substantially different from what would normally be expected from that type of account

**EXAMPLE**: check-cashing business that deposits large sums of cash instead of withdrawing cash for cashing checks
Surveillance Monitoring:

• Authority to establish or change filters should be clearly defined & should require the approval of BSA officer or senior management

• Document and be able to explain filtering criteria, thresholds used, & how both are appropriate for your risks
Surveillance Monitoring:

- Management should periodically review filtering criteria & thresholds established
  - Are they still effective & appropriate for the risk
- Methodology & effectiveness should be independently reviewed & evaluated
  - To ensure that you are detecting potentially suspicious activity
  - Are there any gaps
MANAGING ALERTS
MANAGING ALERTS

• Alert Management is the process used to investigate & evaluate any unusual activity identified.

• Consider all methods of identification & ensure that your suspicious activity monitoring program includes the process to evaluate any unusual activity identified, regardless of method of identification.
MANAGING ALERTS

• Have policies & procedures in place for referring unusual activity from all areas of the bank or business lines to the personnel responsible for evaluation

• Establish a clear & defined escalation process from the point of initial detection to conclusion of the investigation
MANAGING ALERTS

Assign adequate staff to identification, evaluation, & reporting of potentially suspicious activities

– Consider overall risk and volume of transactions
– Experience levels and ongoing training to maintain expertise
– Sufficient internal & external tools to allow them to properly research activities & formulate conclusions
MANAGING ALERTS

Internal research tools

• Access to account systems & account information (Employee Accounts too)

• CDD and EDD information
  – Assist in evaluating if the unusual activity is considered suspicious

External research tools

• Available Internet media search tools, as well those accessible by subscription
MANAGING ALERTS

After research & analysis investigators should:

Document Conclusions
(including recommendation regarding to file or not to file)
MANAGING ALERTS

• When multiple departments are responsible for researching unusual activities, lines of communication must remain open

• Allows multiple departments to gain efficiencies by:
  – sharing information
  – reducing redundancies
  – ensuring all suspicious activity is identified, evaluated, & reported
MANAGING ALERTS

• Required to report activity that may involve money laundering, BSA violations, terrorist financing, & certain other crimes

• However, not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, & various types of fraud)

• Investigation is the responsibility of law enforcement

• When evaluating & completing SAR:
  – To the best of their ability, identify the characteristics of the suspicious activity
SAR DECISION MAKING
SAR DECISION MAKING

After research & analysis is complete

• Forward findings to final decision maker
  – May be individual or committee

• Have policies & procedures for referring unusual activity from all business lines to personnel responsible

• Within procedures, establish clear & defined escalation process from point of initial detection to conclusion of investigation
SAR DECISION MAKING

• Decision maker should have the authority to make the final SAR filing decision

• If committee, should be a clearly defined process to resolve differences of opinion on filing decisions

• Document SAR decisions, including the specific reason for filing or not filing a SAR

• Thorough documentation provides record of SAR decision-making process, including final decisions not to file a SAR
SAR DECISION MAKING

• Decision may be an inherently subjective judgment
• Examiners focus on whether there’s an effective SAR decision-making process, not individual decisions
• Examiners review individual SAR decisions as a way to test effectiveness of monitoring, reporting, & decision-making processes
• However in instances where the institution:
  – Has an established decision-making process
  – Has followed existing policies, procedures, & processes
  – And has determined not to file a SAR

  Should not be criticized for failure to file unless significant or accompanied by evidence of bad faith
SAR COMPLETION & FILING
SAR COMPLETION & FILING

Critical part of SAR monitoring & reporting process

• Policies & procedures to ensure SAR forms are:
  – Filed in a timely manner
  – Are complete and accurate
  – That narrative provides a sufficient description of activity as well as the reason for filing

• Beginning September 12, 2009, institutions that file SARs electronically can receive a Document Control Number as acknowledgement of receipt from FinCEN
Timing of the SAR Filing
SAR COMPLETION & FILING

TIMING:

• No later than 30 calendar days from date of the initial detection of facts that may constitute a basis for filing a SAR

• If no suspect can be identified, time period is extended to 60 days
SAR COMPLETION & FILING

TIMING:

• May need to research transaction, account activity, or other circumstances in order to determine whether to file

• Need for a review of a customer or transactions does not necessarily indicate a need to file a SAR

• Time period for filing starts when 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
TIMING:

• Phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review.

• A variety of legitimate transactions could raise a red flag simply because they are inconsistent with account holder’s normal account activity.

• For example, a real estate purchase or sale, or an inheritance, or a stock sale, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity.
SAR COMPLETION & FILING

TIMING:

• Your monitoring system, alerts, or initial discovery of information on a report 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 determination is made that the transaction under review is “suspicious.”
TIMING:

• Expeditious review is recommended & helps law enforcement

• Complete reviews in a reasonable period of time

• What is "reasonable" will vary according to facts & circumstances of what is being reviewed & the effectiveness of the SAR monitoring, reporting, & decision-making process

• **Key factor:** Are there established & adequate procedures for reviewing & assessing facts & circumstances identified as potentially suspicious, & are they being followed
TIMING:

- For situations requiring immediate attention, in addition to a timely SAR, immediately notify, by phone, "appropriate law enforcement authority" & as necessary, your primary regulator.

- "Appropriate law enforcement authority" is generally the local office of IRS Criminal Investigation Division or FBI.

- Notifying law enforcement of a suspicious activity does not relieve an institution of its obligation to file a SAR.
SAR Quality
Quality:

- Required to file SARs that are complete, thorough, & timely
- Include all known subject information
- Importance of accuracy cannot be overstated
- Inaccurate information, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible
Quality:

- May be legitimate reasons why info is not provided in SAR, such as when filer does not have the information (missing birth date or SSN).
- Thorough & complete narrative may make the difference in determining whether possible criminal nature is clearly understood by law enforcement.
- SAR narrative section is the only area summarizing suspicious activity, this section is critical.
- Failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.
SAR COMPLETION & FILING

SAR Narratives:

• Subjective: Examiners generally will not criticize interpretation of facts
• Ensure narratives are complete & thoroughly describe the extent & nature of the suspicious activity
• No attachments can be sent or stored in the BSA-reporting database (regardless of paper filing or e-filing)
• Guidance available in Appendix L of the FFIEC BSA Exam manual (“SAR Quality Guidance”)
Repetitive SARs (SAR Renewals)
SAR Filing on Continuing Activity

• One purpose of filing is to identify potential violations of law to appropriate law enforcement for investigation
• Objective is accomplished by filing the SAR that identifies the activity of concern
• If this activity continues over a period of time, this needs to be made known to law enforcement and federal banking agencies
• FinCEN’s guidelines suggest that institutions should report continuing suspicious activity by filing a report at least every 90 days
• This practice will notify law enforcement of the continuing nature of the activity
• SAR renewals remind the institution that it should continue to review the activity to determine whether other actions may be appropriate, such as:
  – Determining that it is necessary to terminate a relationship with a customer or employee who is the subject of the filing
SAR Filing on Continuing Activity

• Law enforcement may want accounts to remain open even if there is suspicious or potential criminal activity in connection with those accounts

• If they request that account remains open, institution should ask for a written request

• Request should indicate that agency has requested the account remain open & the purpose & duration

• Ultimate decision to maintain or close an account should be made by each financial institution in accordance with its own standards and guidelines
SAR Filing on Continuing Activity

Add to current policies and procedures when to escalate issues or problems identified as the result of repeat SAR filings on accounts

• Procedures should include:
  – Review by senior management & legal staff (e.g., BSA compliance officer or SAR committee)
  – Criteria for when analysis of the overall customer relationship is necessary
  – Criteria for whether & if so, when, to close the account
  – Criteria for when to notify law enforcement
Record Retention
SAR COMPLETION & FILING

Retention & Supporting Documentation:

• Retain copy of SAR & supporting documentation for 5 years from date of filing: Electronic or Paper.
• Provide all documentation supporting the filing of a SAR upon request to FinCEN or appropriate law enforcement or federal banking agency.
• “Supporting documentation” refers to all documents or records that assisted the institution in making the determination that a SAR was required.
• No legal process is required for FinCEN or appropriate law enforcement or federal banking agency to obtain copies of the supporting documentation.
Notify Board of Directors:

- Notify board of directors or appropriate board committee
- No mandated format or frequency; monthly, quarterly
- May, but not required to, provide actual copies of SARs
- Or provide summaries, tables of SARs filed for specific violation types, or other forms of notification
- Regardless of format, sufficient & timely information must be provided on SAR filings to the board or appropriate committee in order for them to fulfill their fiduciary duties
SAR COMPLETION & FILING

Sharing with Head Offices & Controlling Companies

Institutions may share SARs with head offices & controlling companies, whether in U.S. or abroad

Controlling company defined as:

- Bank holding company (BHC)
- Savings & loan holding company
- Company having the power, directly or indirectly, to direct management policies of an industrial loan company or a parent company or to vote 25% or more of any class of voting shares of an industrial loan company or parent company
SAR COMPLETION & FILING

Sharing With Head Offices & Controlling Companies:

Guidance confirms:

- U.S. branch or agency of a foreign bank may share SAR with head office outside United States
- U.S. bank may share SAR with controlling companies whether domestic or foreign
- Maintain appropriate arrangements to protect the confidentiality of SARs

And FinCEN advisory passed 11/23/10:

*Clarifies & strengthens the scope of SAR confidentiality, & expands the ability of certain financial institutions to share SAR information with most affiliates*
Prohibition of SAR Disclosure
Prohibition of SAR Disclosure:

- 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.
- So if subpoenaed or requested to disclose a SAR or information contained in a SAR, (except when disclosure is requested by FinCEN or an appropriate law enforcement or federal banking agency)
  - **Decline** to produce the SAR and
  - **Decline** to provide any information that would disclose that a SAR has been prepared or filed

(1 CFR 103.18(e) and 31 USC 5318(g)(2))
Convicted for SAR Disclosure

January 10, 2011: Riverside, CA

• Frank Mendoza, former Chase Bank official, faces up to 95 years in prison
• Convicted of disclosing the existence of a suspicious activity report to the suspect
• Mendoza, a loss mitigation specialist, approached subject of the SAR & disclosed existence of SAR & suggested suspect pay him $25K for more information about the investigation

http://losangeles.fbi.gov/dojpressrel/pressrel11/la011111.htm
Prohibition of SAR Disclosure:

• FinCEN & your federal banking agency should be notified of any request

• Both agencies take the position that banks’ internal controls for the filing of SARs should minimize the risks of disclosure
Roll the 4 Elements of an Effective Suspicious Activity Monitoring Program Into Your Desktop Procedures
# Table of Contents

I. **INTRODUCTION** .............................................................................................................................................. 3  
   General guidelines on BSA Monitoring Responsibilities ......................................................................................... 3

II. **IDENTIFICATION OF SUSPICIOUS ACTIVITY** .............................................................................................. 3

III. **MANAGING ALERTS** ....................................................................................................................................... 7

IV. **CASE MANAGEMENT- (Documentation)** ....................................................................................................... 7  
    a. Online “Proof of Review” ............................................................................................................................... 7  
    b. Comments ....................................................................................................................................................... 8  
    c. Initiating an Investigation: “SAR Grouping” .................................................................................................. 9

V. **SAR DECISION MAKING PROCESS** .................................................................................................................. 11  
    a. Clearing a SAR Grouping – “No SAR” decisions: ............................................................................................. 11  
    b. To Initiate SAR filing from SAR Evaluation: .................................................................................................. 12

VI. **SAR COMPLETION AND FILING** .................................................................................................................... 13

VII. **RISK RATING OF CUSTOMERS** ................................................................................................................... 13

VIII. **RE-EVALUATION OF RISK SCORES** ............................................................................................................ 14

IX. **REVIEW OF HIGH RISK ACCOUNTS** .............................................................................................................. 15  
    a. 90 day Review................................................................................................................................................... 15  
    b. Other Enhanced Due Diligence (EDD) Procedures for High Risk Customers .................................................. 16  
    d. Over-rides......................................................................................................................................................... 17
Thank You!
Maleka Ali, CAMS
Banker’s Toolbox
Manager/Education & Consulting