Importance of Monitoring Suspicious Activity

2016 BSA/AML Conference
April 14, 2016
Agenda

- Why do we monitor for Suspicious Activity?
- What is Suspicious Activity?
- Ways to Identify and Monitor Suspicious Activity
- Money Laundering Red Flags
- How Should Your Bank Monitor Suspicious Activity?
Why Do We Monitor For Suspicious Activity?
Monitoring for Suspicious Activity

- **Federal Regulation:**
  - FDIC 12 CFR 353
  - Federal Reserve 12 CFR 208.62
  - OCC 12 CFR 21.11
  - NCUA 12 CFE 748
  - FinCEN 31 CFR 1020.320

- **Risk of CMPs**

- **Law Enforcement**
Investigations Assisted by FinCEN Data

- Proactive SAR Review Uncovers $15 Million Securities Conversion Scheme
- Case for Mortgage Fraud Involving Straw Buyers Supported by SARs
- SAR Filing Locates Check Kiting Suspect
- Detailed SAR Narratives Help Uncover Cigarette Smuggling Operation
- SARs Lead to Discovery of $1.8 Million Hidden in House
- One Hundred SARs Help Outline Size and Scope of Fraudulent Mortgage Elimination Scheme
- SARs Identify Internal Fraud at Local Bank
- SAR Filings Reveal Methamphetamine Production Ring

- SAR Referral Leads to the Discovery of a $100 Million Mortgage Fraud and Foreclosure Rescue Scheme
- Bank Secrecy Act Data Leads to Seizure of $18 Million
- SARs Help Bust $1 Million Drug Ring Led by Significantly Older Student
- Proactive Review of SARs Leads to Long Prison Sentences for Drug Traffickers
- SARs Reveal Multi-Million Dollar Illicit Business
- SAR Filing Leads to 125-Count Indictment in $2.7 Million Embezzlement Case
What Is Suspicious Activity?
What is Suspicious Activity?

Definition of Suspicious Activity:

- **Merriam-Webster Dictionary says Suspicious is:** causing a feeling that something is wrong or that someone is behaving wrongly: causing suspicion

- **Merriam-Webster Dictionary says Activity is:** the state of being active: behavior or actions of a particular kind
  - something that is done as work or for a particular purpose
Ways To Identify and Monitor Suspicious Activity
Key to an Effective Suspicious Activity Monitoring Program

- Know your Customer
  - CIP
  - Customer Due Diligence
  - EDD
Systems to Identify, Research and Report Suspicious Activity

- Risk-based
- Staff
- Monitor
- Policy/Procedures
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
- Monitoring and SAR Filing on Continuing Activity
Identification of Unusual Activity

1. Employees

2. Law Enforcement

3. Management Information Systems (MIS)
1. Employee Identification

- Day-to-day operations
- All departments
- Training
- Policies
2. Law Enforcement

- National Security Letter (NSL)
- Section 314(a)
3. Management Information Systems

3 Types of Anti-Money Laundering MIS

I. Record-Keeping Systems

II. Transaction/Account Monitoring Systems

III. Transaction Filtering Systems
Record-Keeping Systems

- System tracks historical information
- “After-the-Fact”
- Most Basic AML System
- Manual review of MIS generated reports
Record-Keeping Systems

- Specific Targets
- Filtering
- Thresholds
- Frequency
- Examples
  - Currency Activity Reports
  - Funds Transfer Reports
  - Monetary Instrument Sales Reports
Currency Activity Reports

- Currency activity including multiple transactions over $10,000.
- Currency activity below $10,000.
- 3 or more cash-in transactions in the last 30 days – each more than $7,999
- Transactions aggregated by customer name, TIN or CIF.
Funds Transfer Records

- Funds Transfers over $3,000
- Volume
  - Manual review vs automated review
- Filtering Criteria
Manual Transaction Monitoring - Checks

- Monetary Instrument Records
  - Cashier’s checks, official bank checks, money orders or traveler’s checks in amounts of $3,000 to $10,000
  - Review activity for an extended period of time (30, 60, 90 days)
Other areas

- Tax refunds
- Social security deposits
- Account holders with a non-local address
- High volume of activity and low balance
- Disbursement of CDs by multiple bank checks
- Early redemption of CDs
- Funds deposited into several accounts, transferred to another account, and then transferred outside of the US
Other areas (Cont.)

- Significant balance change reports
- Non-Resident Alien Reports
- Inconsistent deposit and withdrawal activity
- ATM Withdrawals of 20 or more
- New Products or Services
- Loan payments by third parties
- Incoming and outgoing wires in similar small dollar amounts
- Business customers with the same address
Automated Transaction Monitoring

Types of Systems

- Rule Based
- Artificial Intelligence
- Combination
Automated Transaction Monitoring – Rule Based

- Based on Standard Rules
- Rules Remain Static
  - Unless Physically Changed in the System
- Detect Transactions Outside Expected Norm
- Look at Each Transaction Individually
- Examples of Rules that Generate Alerts
Artificial Intelligence (AI)

- Learns a customer’s behavior patterns
- Detects *Unusual* Patterns of Activity or Customer Activity
- Use Various Approaches to Identify Suspicious Activities
- Analysis Changes over Time with Activity Patterns
Automated Transaction Monitoring – Artificial Intelligence (Cont.)

- Analyzes transactions based on business line or past transaction history
- Inconsistent activity generates alerts
- Some systems compare customer transactions to their own history AND to its peers.
Automated Transaction Monitoring – Artificial Intelligence (Cont.)

- May be used in conjunction with rule-based logic
- Can be set to review individual account histories
- Can detect behaviors indicating money laundering between accounts, which are not obvious to rule or profile-based applications.
Automated Transaction Monitoring - Authority/Change Management

- Clearly define authority to establish/change activity profiles
- Require BSA officer or senior management approvals for changes
- Document/explain filtering criteria, thresholds, and appropriateness for bank risk
- Periodically review filtering criteria and thresholds
- Independently validate programming methodology
Checks Customer Names Against “Lists”

- OFAC
- Politically Exposed Persons
- 314(a) Lists
- Internal Lists
- 311 Special Measures
Money Laundering Red Flags
What is Money Laundering?
Money Laundering Red Flags – General

- Refusal or reluctance to proceed with a transaction or abruptly withdrawing a transaction
- Customer refusal or reluctance to provide information or identification
- Structured or recurring, non-reportable transactions
- Multiple third parties conducting separate, but related, non-reportable transactions
- Even dollar amount transactions
- Transactions structured to lose the paper trail
- Significant increases in the number or amount of transactions
- Transactions which are not consistent with the customer’s business, occupation, or income level
- Transactions by non-account holders
Money Laundering Red Flags – Cash Management

- Change in currency shipment patterns
- Large increase in the cash supply
- Currency shipments to or from remote locations
- Significant exchanges of small denomination bills for large denomination bills
- Significant requirement for large bills
- International cash shipments funded by multiple monetary instruments
- Other unusual domestic or international shipments
- Frequent cash shipments with no apparent business reason
Money Laundering Red Flags - Currency

- Unusual exchange of denominations.
- Check cashing companies.
- Unusual exchange by a check cashing service.
- Suspicious movement of funds.
Money Laundering Red Flags – Deposit Accounts

- Minimal, vague or fictitious information provided
- Lack of references or identification
- Non-local address
- Customers with multiple accounts
- Frequent deposits or withdrawals with no apparent business source
- Multiple accounts with numerous deposits under $10,000
- Numerous deposits under $10,000 in a short period of time
- Accounts with a high volume of activity and low balances
- Large deposits and balances
- Deposits and immediate requests for wire transfers or cash shipments
Money Laundering Red Flags – Deposit Accounts (Cont.)

- Numerous deposits of small incoming wires or monetary instruments, followed by a large outgoing wire
- Accounts used as a temporary repository for funds
- Funds deposited into several accounts, transferred to another account, and then transferred outside of the U.S.
- Disbursement of certificates of deposit by multiple bank checks
- Early redemption of certificates of deposits
- Sudden, unexplained increase in account activity or balance
- Limited use of services
- Inconsistent deposit and withdrawal activity
- Strapped currency
- Client, trust and escrow accounts
Money Laundering Red Flags - Lending

- Certificates of deposits used as collateral
- Sudden/unexpected payment on loans
- Reluctance to provide the purpose of the loan or the stated purpose is ambiguous
- Inconsistent or inappropriate use of loan proceeds
- Overnight loans
- Loan payments by third parties
- Loan proceeds used to purchase property in the name of a third party, or collateral pledged by a third party
- Permanent mortgage financing with an unusually short maturity, particularly in the case of large mortgages
- Structured down payments or escrow money transactions
- Attempt to sever the paper trail
- Wire transfer of loan proceeds
- Disbursement of loan proceeds by multiple bank checks
- Loans to companies outside the U.S.
- Financial statement
Money Laundering Red Flags – Monetary Instruments

- Structured purchases of monetary instruments
- Replacement of monetary instruments
- Frequent purchase of monetary instruments without apparent legitimate reason
- Incomplete or fictitious information
- Large cash amounts
Money Laundering Red Flags – Safe Deposit Boxes

- Frequent visits
- Out-of-area customers
- Change in safe deposit box traffic pattern
- Large amounts of cash maintained in a safe deposit box
- Multiple safe deposit boxes
Money Laundering Red Flags – Wire Transfers

- Wire transfers to countries widely considered “secrecy havens”
- Incoming/outgoing wire transfers with instructions to the receiving institution to pay upon proper identification
- Outgoing wire transfers requested by non-account holders
- Frequent wire transfers with no apparent business reason
- High volume of wire transfers with low account balances
- Incoming and outgoing wires in similar dollar amounts
- Large wires by customers operating a cash business
- Cash or bearer instruments used to fund wire transfers
- Unusual transaction by correspondent financial institutions
- International funds transfer(s) which are not consistent with the customer’s business
- International transfers funded by multiple monetary instruments
- Other unusual domestic or international funds transfers
- No change in form of currency
Money Laundering Red Flags: Other

- Questions or discussions on how to avoid reporting/recordkeeping
- Customer attempt to influence a bank employee not to file a report
- Lavish lifestyles of customers or bank employees
- Short-term or no vacations
- Circumvention of internal control procedures
- Incorrect or incomplete CTRs
How Should Your Bank Monitor Suspicious Activity?
Conclusion

How Should Your Bank Monitor Suspicious Activity?

Answer:
Take Action

- Review your current methods to monitor suspicious activity
- Can these methods/processed be enhanced?
- Talk with your vendors
- Obtain additional reports
Resources

- 2014 FFIEC BSA/AML Examination Manual
- Section 8 of the FDIC Risk Management Manual of Examination Policies
- Federal Regulation:
  - FDIC 12 CFR 353
  - Federal Reserve 12 CFR 208.62
  - OCC 12 CFR 21.11
  - NCUA 12 CFE 748
  - FinCEN 31 CFR 1020.320