Advanced BSA Topics

BSA Graduate School

January 2018

Consultants to the Financial Industry
Young & Associates, Inc.
121 E. Main Street
P.O. Box 711
Kent, OH 44240
Phone: 330.678.0524
Fax: 330.678.6219
www.younginc.com

Table of Contents

Part 1: General Advanced Topics

Section 1: Overview and Introduction

This course has been designed with the understanding that each attendee has a general knowledge base of basic BSA components. Therefore, we have not included the core elements of BSA rules in this manual. Some BSA elements, however, are not specific to every organization and are more specialized, or advanced, in nature. In this section, we will specifically address some of these advanced topics as follows:

- Privately Owned ATMs
- Politically Exposed Persons
- Management Information Systems
- Independent Testing
- Culture of BSA/AML Program

The FFIEC BSA Examination Manual provides interagency guidance for mitigating the risk associated with most of the above items. Therefore, we have built this portion of the manual from that guidance, as applicable. The many of the following pages include applicable sections from the FFIEC BSA Examination Manual.

Section 2: Privately Owned Automated Teller Machines

Overview

Each financial institution should establish systems to manage the risks associated with privately owned automated teller machines (ATM) and Independent Sales Organization (ISO) relationships. In addition, those in BSA management roles must have the ability to implement effective due diligence, monitoring, and reporting systems related to these items.

Privately owned ATMs are particularly susceptible to money laundering and fraud. Operators of these ATMs are often included within the definition of an ISO.

Privately owned ATMs are typically found in convenience stores, bars, restaurants, grocery stores, or check cashing establishments. Some ISOs are large-scale operators, but many privately owned ATMs are owned by the proprietors of the establishments in which they are located. Most dispense currency, but some dispense only a paper receipt (scrip) that the customer exchanges for currency or goods. Fees and surcharges for withdrawals, coupled with additional business generated by customer access to an ATM, make the operation of a privately owned ATM profitable.

ISOs link their ATMs to an ATM transaction network. The ATM network routes transaction data to the customer's bank to debit the customer's account and ultimately credit the ISO's account, which could be located at a bank anywhere in the world. Payments to the ISO's account are typically made through the automated clearinghouse (ACH) system.

Sponsoring Bank

Some electronic funds transfers (EFT) or point-of-sale (POS) networks require an ISO to be sponsored by a member of the network (sponsoring bank). The sponsoring bank and the ISO are subject to all network rules. The sponsoring bank is also charged with ensuring the ISO abides by all network rules. Therefore, the sponsoring bank should conduct proper due diligence on the ISO and maintain adequate documentation to ensure that the sponsored ISO complies with all network rules.

Risk Factors

Most states do not currently register, limit ownership, monitor, or examine privately owned ATMs or their ISOs the provider of the ATM transaction network and the sponsoring bank should be conducting adequate due diligence on the ISO, actual practices may vary. Furthermore, the provider may not be aware of ATM or ISO ownership changes after an ATM contract has already been established. As a result, many privately owned ATMs have been involved in, or are susceptible to, money laundering schemes, identity theft, outright theft of the ATM currency, and fraud. Consequently, privately owned ATMs and their ISOs pose increased risk and should be treated accordingly by banks doing business with them.

Due diligence becomes more of a challenge when ISOs sell ATMs to, or subcontract with, third- and fourth-level companies ("sub-ISOs") whose existence may be unknown to the

sponsoring bank. When an ISO contracts with or sells ATMs to sub-ISOs, the sponsoring bank may not know who actually owns the ATM. Accordingly, sub-ISOs may own and operate ATMs that remain virtually invisible to the sponsoring bank.

Some privately owned ATMs are managed by a vault currency servicer that provides armored car currency delivery, replenishes the ATM with currency, and arranges for insurance against theft and damage. Many ISOs, however, manage and maintain their own machines, including the replenishment of currency. Banks may also provide currency to ISOs under a lending agreement, which exposes those banks to various risks, including reputation and credit risk.

Money laundering can occur through privately owned ATMs when an ATM is replenished with illicit currency that is subsequently withdrawn by legitimate customers. This process results in ACH deposits to the ISO's account that appear as legitimate business transactions. Consequently, all three phases of money laundering (placement, layering, and integration) can occur simultaneously. Money launderers may also collude with merchants and previously legitimate ISOs to provide illicit currency to the ATMs at a discount.

Risk Mitigation

Banks should implement appropriate policies, procedures, and processes, including appropriate due diligence and suspicious activity monitoring, to address risks with ISO customers. At a minimum, these policies, procedures, and processes should include:

- Appropriate risk-based due diligence on the ISO, through a review of corporate documentation, licenses, permits, contracts, or references.
- Review of public databases to identify potential problems or concerns with the ISO or principal owners.
- Understanding the ISO's controls for currency servicing arrangements for privately owned ATMs, including source of replenishment currency.
- Documentation of the locations of privately owned ATMs and determination of the ISO's target geographic market.
- Expected account activity, including currency withdrawals.

Because of these risks, ISO due diligence beyond the minimum CIP requirements is important. Banks should also perform due diligence on ATM owners and sub-ISOs, as appropriate. This due diligence may include:

- Reviewing corporate documentation, licenses, permits, contracts, or references, including the ATM transaction provider contract.
- Reviewing public databases for information on the ATM owners.
- Obtaining the addresses of all ATM locations, ascertain the types of businesses in which the ATMs are located, and identify targeted demographics.
- Determining expected ATM activity levels, including currency withdrawals.

- Ascertaining the sources of currency for the ATMs by reviewing copies of armored car contracts, lending arrangements, or any other documentation, as appropriate.
- Obtaining information from the ISO regarding due diligence on its sub-ISO arrangements, such as the number and location of the ATMs, transaction volume, dollar volume, and source of replenishment currency.

Section 3: Politically Exposed Persons

Overview

Each financial institution should establish systems to manage the risks associated with senior foreign political figures, often referred to as "politically exposed persons" (PEP). BSA managers must possess the ability to implement effective risk-based due diligence, monitoring, and reporting systems for these persons.

Banks should take all reasonable steps to ensure that they do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior foreign political figures, their families, and their associates. Because the risks presented by PEPs will vary by customer, product/service, country, and industry, identifying, monitoring, and designing controls for these accounts and transactions should be risk-based.

The term "politically exposed person" generally includes a current or former senior foreign political figure, their immediate family, and their close associates. Interagency guidance issued in January 2001 offers banks resources that can help them to determine whether an individual is a PEP. More specifically:

- A "senior foreign political figure" is a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. In addition, a senior foreign political figure includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior foreign political figure.
- The "immediate family" of a senior foreign political figure typically includes the figure's parents, siblings, spouse, children, and in-laws.
- A "close associate" of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with the senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure.

The definition of senior official or executive must remain sufficiently flexible to capture the range of individuals who, by virtue of their office or position, potentially pose a risk that their funds may be the proceeds of foreign corruption. Titles alone may not provide sufficient information to determine if an individual is a PEP, because governments are organized differently from jurisdiction to jurisdiction. In those cases when a bank files a SAR concerning a transaction that may involve the proceeds of foreign corruption, FinCEN has instructed banks to include the term "foreign corruption" in the narrative portion of the SAR. Banks should establish risk-based controls and procedures that include reasonable steps to ascertain the status of an individual as a PEP and to conduct risk-based scrutiny of accounts held by these individuals. Risk will vary depending on other factors such as products and services used and size or complexity of the account relationship. Banks also should consider various factors when determining if an individual is a PEP including:

- Official responsibilities of the individual's office.
- Nature of the title (e.g., honorary or salaried).
- Level and nature of authority or influence over government activities or other officials.
- Access to significant government assets or funds.

In determining the acceptability of higher-risk accounts, a bank should be able to obtain sufficient information to determine whether an individual is or is not a PEP. For example, when conducting due diligence on a higher-risk account, it would be usual for a bank to review a customer's income sources, financial information, and professional background. These factors would likely require some review of past and present employment as well as general references that may identify a customer's status as a PEP. Moreover, a bank should always keep in mind that identification of a customer's status as a PEP should not automatically result in a higher-risk determination; it is only one factor the bank should consider in assessing the risk of a relationship.

Ascertaining whether a customer has a close association with a senior foreign political figure can be difficult, although focusing on those relationships that are "widely and publicly known" provides a reasonable limitation on expectations to identify close associates as PEPs. However, banks that have actual knowledge of a close association should consider their customer a PEP, even if such association is not otherwise widely or publicly known. Banks are expected to follow reasonable steps to ascertain the status of an individual, and the federal banking agencies and FinCEN recognize that these steps may not uncover all close associations.

Risk Factors

In high-profile cases over the past few years, PEPs have used banks as conduits for their illegal activities, including corruption, bribery, and money laundering. However, not all PEPs present the same level of risk. This risk will vary depending on numerous factors, including the PEP's geographic location, industry, or sector, position, and level or nature of influence or authority. Risk may also vary depending on factors such as the purpose of the account, the actual or anticipated activity, products and services used, and size or complexity of the account relationship.

As a result of these factors, some PEPs may be lower risk and some may be higher risk for foreign corruption or money laundering. Banks that conduct business with dishonest PEPs face substantial reputational risk, additional regulatory scrutiny, and possible supervisory action. Red flags regarding transactions that may be related to the proceeds of foreign corruption are listed in the January 2001 interagency guidance. Banks also should be alert to a PEP's access to, and control or influence over, government or corporate accounts; the level of involvement of intermediaries, vendors, shippers, and agents in the industry or sector in which the PEP operates; and the improper use of corporate vehicles and other legal entities to obscure ownership.

Risk Mitigation

Banks should exercise reasonable judgment in designing and implementing policies, procedures, and processes regarding PEPs. Banks should obtain risk-based due diligence information on PEPs and establish policies, procedures, and processes that provide for appropriate scrutiny and monitoring. Having appropriate risk-based account opening procedures for large-dollar or higher-risk products and services is critical. The opening of an account is the prime opportunity for the bank to gather information for all customers, including PEPs. Commensurate with the identified level of risk, due diligence procedures should include, but are not necessarily limited to, the following:

- Identify the accountholder and beneficial owner, including the nominal and beneficial owners of companies, trusts, partnerships, private investment companies, or other legal entities that are accountholders.
- Seek information directly from the account holder and beneficial owner regarding possible PEP status.
- Identify the accountholder's and beneficial owner's country(ies) of residence and the level of risk for corruption and money laundering associated with these jurisdictions.
- Obtain information regarding employment, including industry and sector and the level of risk for corruption associated with the industries and sectors.
- Check references, as appropriate, to determine whether the account holder and beneficial owner is or has been a PEP.
- Identify the account holder's and beneficial owner's source of wealth and funds.
- Obtain information on immediate family members or close associates either having transaction authority over the account or benefiting from transactions conducted through the account.
- Determine the purpose of the account and the expected volume and nature of account activity.
- Make reasonable efforts to review public sources of information. These sources will vary depending upon each situation; however, banks should check the accountholder and any beneficial owners of legal entities against reasonably accessible public sources of information (e.g., government databases, major news publications, commercial databases and other databases available on the Internet, as appropriate).

PEP accounts are not limited to large or internationally focused banks. A PEP can open an account at any bank, regardless of its size or location. Banks should have risk-based procedures for identifying PEP accounts and assessing the degree of risks involved, which will vary. Management should be involved in the decision to accept a PEP account. If management determines after-the-fact that an account is a PEP account, it should evaluate the risks and take appropriate steps. The bank should exercise additional, reasonable due diligence with regard to such accounts. For example, the bank may increase reference inquiries, obtain additional background information on the PEP from branches or correspondents operating in the client's home country, and make reasonable efforts to consult publicly available information sources.

Ongoing risk-based monitoring of PEP accounts is critical to ensuring that the accounts are being used as anticipated. Refer to core overview section, "Private Banking Due Diligence Program (Non-U.S. Persons)," pages 130 to 134, for expectations regarding private banking relationships with PEPs.

Section 4: Management Information Systems

OverviewAs BSA monitoring has evolved over the years, Banks have decreased their reliance upon manual data analysis and have increasingly utilized automated systems to assist in the data analysis process. Rather than leaving Bankers to conduct cumbersome manual reviews of raw data, management information systems (MIS) automatically run various queries, statistical analysis, and mathematical algorithms that provide management with an efficient and often effective way to review their data. An MIS is typically utilized in one of two ways to assist management in data analysis:

1. As a Manual Transaction Monitoring System
2. As an Automated Account Monitoring System

For Banks that utilize a Manual Transaction Monitoring System in their BSA program, the MIS assists management in the analysis of data through the creation of certain reports. These reports, often generated through utilization of filtering models by various systems, such as the Bank's Core Processing System, help to organize data into a manageable form. Popular reports that are often utilized and reviewed in a Manual Transaction Monitoring System are large currency transaction reports, suspect kiting reports, funds transfer reports, monetary instrument sales reports, significant balance change reports, nonsufficient funds (NSF) reports, and Wire Transfer Reports. While these reports help to manage the Bank's Data, the identification and recording of certain qualified transactions often remains a manual process for the Bank.

Alternatively, an Automated Account Monitoring System can help to take the BSA review function to the next level; it can assist a bank in identifying and recording certain qualified transactions. An Automated Account Monitoring System is usually a separate product the Bank must purchase and implement through the utilization of a third-party vendor. Alternatively, a Bank could develop an Automated Account Monitoring System internally using either an in-house programmer or an independent contractor. Regardless of what program is implemented by a Bank, an Automated Account Monitoring System can take a large amount of time and resources to effectively implement. For example, Management must define a large number of parameters and filtering criteria based on its perceived risk tolerance for each applicable area. Additionally, the system must be implemented in a way so that all applicable data is pulled into the system for data analysis.

When banks rely on an MIS for generating reports used to monitor and track certain BSA activities, it is imperative to ensure the utilized systems are working as intended. When implemented, banks often rely heavily upon system-generated reports provided by their MIS. If a bank was to implement an MIS that lacked integrity due to a poor design or improper implementation, significant consequences could occur. For example, if a bank were to open a new branch and not include that branch in its large currency transaction reports (LTCR) on its system specifications, the employee reviewing the LTCR would not be able to identify qualified CTR transactions from this branch. Therefore, even if the employee were to conduct a thorough review of the LTCR, the Bank's program would have significant deficiencies due to the improper implementation of specifications of the Management Information System in which the Bank relied upon.

Types of Monitoring Systems

As referenced previously, there are generally two different types of monitoring systems:

1. Transaction Monitoring (Manual Transaction Monitoring)
2. Surveillance Monitoring (Automated Account Monitoring)

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, 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.

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, tax 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, will significantly enhance a bank's ability to identify and evaluate unusual currency transactions.

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. These rules are often based on statistical analysis and complex algorithms that are automatically calculated and result in a "flag" for the bank to review.

Many of these systems 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 clearinghouse (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 and should generally require the approval of the BSA compliance officer or senior management. Controls should ensure limited access to the monitoring system. Management should document or be able to explain filtering criteria, thresholds used, and how both are appropriate for the bank's risks. Management should also periodically review 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.

Evaluating an MIS

To test the accuracy and integrity of the Bank's MIS, three main elements of the MIS can be reviewed:

1. The implementation of the MIS such as parameters, settings and filter criteria
2. The programming of the methodology used in the MIS
3. MIS Transactions (Testing)

Implementation of the MIS

To ensure the accuracy and integrity of Management Information Systems, a bank may choose to conduct a risk-based review of the implementation of applicable systems. In conducting this review, one would review the various account settings, parameters, and filtering criteria that can be controlled by the Bank and subsequently affect the level of monitoring performed by the organization. Properly implemented parameters, settings and filtering criteria provides for an effective Management Information System. Alternatively, poorly implemented settings, parameters and filtering criteria will either provide gaps within the institutions BSA program or create inefficiencies do to excessive monitoring for the level of perceived risk.

For the review, one should, at a minimum, ensure all branches and applicable employees (tellers) are included on the account parameters. Additionally, the MIS can be tested to ensure applicable types of cash deposits, such as loan payments, gift card purchases, and ATM deposits,

are included in the account settings. Furthermore, a general risk-based review of certain parameters, settings, and filtering criteria can be utilized to identify those that appear to be inconsistent with similar items deployed by the Bank.

MIS Methodology

To ensure the accuracy and integrity of management information systems, a bank may choose to conduct a risk-based review of the methodology deployed to operate applicable systems, reports, and prompts.

Manual Systems. For a Manual Transaction Monitoring System, the review would generally cover a combination of system filters for generating applicable reports as well as the Bank's procedures for reviewing the data generated from these reports. Additionally, a due diligence review process, as appropriate, should be utilized for reviewing the management information systems utilized in the Bank's Manual Transaction Monitoring System.

Automated Systems. For an Automated Transaction Monitoring System, the review would generally ensure the appropriateness of the account settings. Of particular concern should be the effectiveness of the system settings. For example, if a bank is utilizing settings that are too broad, employees may be conducting more work than is necessary, meaning that excessive time is actually being spent on low-risk items. Appropriate utilization of system parameters will ensure that employees retain a risk-based approach to BSA monitoring activities.

Specifically, a reviewer can test the total number of alerts identified by the automated system and compare that number with the number of both SARs considered but not filed and filed SARs. For example, if the Bank is managing over a hundred alerts a day, but at the end of the year only considers and files SARs from front-line employee referrals, the automated monitoring system would not appear to be effective as the amount of work utilized to handle system alerts would not be resulting in effective SAR identification.

On the other hand, if the Bank is managing 15 alerts a day and also filing 3 SARs a month from system identified alerts (not including front line employee referrals), a reviewer may find that the system parameters to be appropriate. As the parameters of an Automated Transaction Monitoring System are often very complex, banks may wish to contact the designer of the system (third-party vendor) and request assistance in evaluating and establishing appropriate parameters.

MIS Transaction Testing

As another step in ensuring the accuracy and integrity of management information systems, a detailed review of select account transactions may be performed. In conjunction with a general overview of the transaction process, this detailed review includes following a transaction from the initial ticket at the teller window to all applicable queries, reports, and reviews. A review may include "expanded transaction testing" to further ensure the accuracy and integrity of the Bank's management information systems. As an example, this expanded review could look at either two (2) transactions per banking branch or it can be customized depending on the needs of the bank.

Overall Assessment of the MIS

When conducting a review of a bank's Management Information System, a reviewer will generally provide an assessment on the overall accuracy and integrity of the Bank's management information systems by providing a specific statement as the overall effectiveness.

At Young & Associates, Inc., we generally will utilize one of the following ratings:

- ***Satisfactory*** – A bank with a satisfactory rating appears to have an MIS that is sufficient for the size and complexity of the organization.
- ***Needs Improvement*** – A bank with a rating of Needs Improvement appears to have a few items that warrant enhancement. While these items do deteriorate the accuracy and integrity of the Bank's MIS, the Bank does retain sufficient levels of appropriateness in several other areas leaving some level of accuracy and integrity for the MIS.
- ***Significant Deficiencies*** – A bank with a rating of Significant Deficiencies has a large number of identified deficiencies that significantly compromises the accuracy and integrity of the Bank's MIS.

Section 5: Independent Testing

Independent testing (audit) is a key element of an effective BSA program and should be conducted by the internal audit department, outside auditors, consultants, or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, a sound practice is for the bank to conduct independent testing generally every 12 to 18 months, commensurate with the BSA/AML risk profile of the bank. Banks that do not employ outside auditors or consultants or have internal audit departments may comply with this requirement by using qualified persons who are not involved in the function being tested. The persons conducting the BSA/AML testing should report directly to the board of directors or to a designated board committee comprised primarily or completely of outside directors.

Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with the BSA, and evaluate pertinent management information systems (see the MIS section of this manual). The audit should be risk based and evaluate the quality of risk management for all banking operations, departments, and subsidiaries. Risk-based audit programs will vary depending on the bank's size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. An effective risk-based auditing program will cover all of the bank's activities. The frequency and depth of each activity's audit will vary according to the activity's risk assessment. Risk-based auditing enables the board of directors and auditors to use the bank's risk assessment to focus the audit scope on the areas of greatest concern. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

Independent testing should, at a minimum, include:

- An evaluation of the overall adequacy and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes. Typically, this evaluation will include an explicit statement about the BSA/AML compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (e.g., an examiner, review auditor, or BSA officer) to reach a conclusion about the overall quality of the BSA/AML compliance program.
- A review of the bank's risk assessment for reasonableness given the bank's risk profile (products, services, customers, entities, and geographic locations).
- Appropriate risk-based transaction testing to verify the bank's adherence to the BSA recordkeeping and reporting requirements (e.g., CIP, SARs, CTRs and CTR exemptions, and information sharing requests).
- An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions, if applicable.
- A review of staff training for adequacy, accuracy, and completeness.
- A review of the effectiveness of the suspicious activity monitoring systems (manual, automated, or a combination) used for BSA/AML compliance. Related reports may include, but are not limited to:
    - Suspicious activity monitoring reports.

  - Large currency aggregation reports.
  - Monetary instrument records.
  - Funds transfer records.
  - Nonsufficient funds (NSF) reports.
  - Large balance fluctuation reports.
  - Account relationship reports.
- An assessment of the overall process for identifying and reporting suspicious activity, including a review of filed or prepared SARs to determine their accuracy, timeliness, completeness, and effectiveness of the bank's policy.
- An assessment of the integrity and accuracy of MIS used in the BSA/AML compliance program. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports.

Auditors should document the audit scope, procedures performed, transaction testing completed, and findings of the review. All audit documentation and workpapers should be available for examiner review. Any violations, policy or procedures exceptions, or other deficiencies noted during the audit should be included in an audit report and reported to the board of directors or a designated committee in a timely manner. The board or designated committee and the audit staff should track audit deficiencies and document corrective actions.

Section 6: Culture of BSA / AML Compliance

Introduction

Shortcomings identified in Anti-Money Laundering (AML) enforcement actions confirm that the culture of an organization is critical to its compliance. Although enforcement actions are specific to the subject financial institution and the characteristics of the situation, certain general lessons could be gleaned from these actions that could be instructive to the leadership of all financial institutions required to comply with the Bank Secrecy Act (BSA). Accordingly, the Financial Crimes Enforcement Network (FinCEN) issues this Advisory to highlight general principles illustrating how financial institutions and their leadership may improve and strengthen organizational compliance with BSA obligations.

Regardless of its size and business model, a financial institution with a poor culture of compliance is likely to have shortcomings in its BSA/AML program. A financial institution can strengthen its BSA/AML compliance culture by ensuring that (1) its leadership actively supports and understands compliance efforts; (2) efforts to manage and mitigate BSA/AML deficiencies and risks are not compromised by revenue interests; (3) relevant information from the various departments within the organization is shared with compliance staff to further BSA/AML efforts; (4) the institution devotes adequate resources to its compliance function; (5) the compliance program is effective by, among other things, ensuring that it is tested by an independent and competent party; and (6) its leadership and staff understand the purpose of its BSA/AML efforts and how its reporting is used. This advisory describes each of these areas in more detail below. Financial institutions should consider how to incorporate the guidance outlined in this advisory in a manner that is commensurate with their risk profile and business model.

FinCEN Guidance to Financial Institutions (FIN-2014-A007)

Leadership Should Be Engaged

A financial institution's leadership is responsible for performance in all areas of the institution including compliance with the BSA. As applicable, an institution's leadership may include its board of directors, senior and executive management, owners and operators. These leaders are responsible for understanding an institution's responsibilities regarding compliance with the BSA and creating a culture of compliance at that institution. The commitment of an organization's leaders should be visible within the organization, as such commitment influences the attitudes of others within the organization.

For a BSA/AML compliance program to be effective, it should have the demonstrable support of the leadership (as appropriate based on the financial institution's size and structure). The institution's leaders should also receive periodic BSA/AML training that is tailored to their roles. In addition to supporting a culture of compliance, an appropriate understanding of BSA/AML obligations and compliance will help an organization's leadership make informed decisions with regard to the allocation of resources to the BSA/ AML function. The leaders of the organization should also remain informed of the state of BSA/AML compliance within the institution.

Compliance Should Not Be Compromised By Revenue Interests

Compliance staff should be empowered with sufficient authority and autonomy to implement an institution's AML program. An institution's interest in revenue should not compromise efforts to effectively manage and mitigate BSA/AML deficiencies and risks, including submission of appropriate and accurate reports to FinCEN. An effective governance structure should allow for the BSA/AML compliance function to work independently and to take any appropriate actions to address and mitigate any risks that may arise from an institution's business line and to file any necessary reports, such as Suspicious Activity Reports (SARs).

For example, for Money Services Businesses (MSBs), principal MSBs often derive a significant percentage of their revenue from the activity of their agents. When principal MSBs learn of possible inappropriate activity by an agent, the activity should be investigated thoroughly and appropriate action taken regardless of the impact on revenue. The findings from the investigation should be considered when determining whether an agent is terminated, and the sales unit should not have express or implied authority to veto the decision because of the agent's sales activity.

Information Should Be Shared Throughout the Organization

Several recent enforcement actions noted that the subject institution had relevant information in its possession that was not made available to BSA/AML compliance staff. This may have resulted from a lack of an appropriate mechanism for sharing information, a lack of appreciation of the significance or relevance of the information to BSA/AML compliance or an intentional decision to prevent compliance officers or staff from having access to the information.

There is information in various departments within a financial institution that may be useful and should be shared with the compliance staff. For example, information developed by those in the organization combating and preventing fraud could also assist a financial institution in complying with its BSA/AML obligations. Similarly, legal departments should alert compliance departments to subpoenas received issued by government agencies to trigger reviews of related customers' risk ratings and account activity for suspicious transactions. Additionally, in a larger organization there may be multiple affiliated institutions that could benefit from sharing of relevant information across the organization.

For instance, in the gaming sector, this principle can be applied to casinos that develop significant information on their gaming customers for purposes of marketing or extending credit. However, that information is derived; it should be provided to the compliance staff to assist in conducting customer due diligence and monitoring customers for suspicious activity. This principle can also be applied to mutual funds that receive transaction information about their customers through a frequent trading monitoring program, or other similar efforts. In those cases, information that could further the BSA/AML compliance efforts of the mutual fund should also be shared with mutual fund staff engaged in BSA/AML compliance.

Leadership Should Provide Adequate Human and Technological Resources

A required element of any BSA/AML compliance program is the designation of an individual responsible for coordinating and monitoring day-to-day compliance with the BSA. The individual should be knowledgeable of the BSA and have sufficient authority to administer the program. For the program to be effective, the institution should devote appropriate support staff to its BSA/AML compliance program based on its risk profile.

The failure of an institution's leaders to devote sufficient staff to the BSA/AML compliance function may lead to other failures. For example, depository institutions, as well as other types of financial institutions, generally have staff that review alerts generated by transaction monitoring systems. Devoting insufficient staff or other resources to this function may result in alerts not being reasonably designed to capture appropriate risks or being dismissed improperly, or create a backlog of alerts that may result in the untimely reporting of suspicious activity.

Appropriate technological resources should also be allocated to BSA/AML compliance. Institutions with higher risk profiles, including those with substantially higher volumes of activity, may need to utilize automated systems for identifying and monitoring suspicious activity.

The Program Should Be Effective and Tested By an Independent and Competent Party

Appropriate involvement of a financial institution's leadership should be, at a minimum, commensurate with the institution's level of BSA/AML risk exposure. Appropriate leadership involvement allows the BSA/AML function to implement an effective compliance program. Components of an effective BSA/AML compliance program additionally include a proper ongoing risk assessment, sound risk-based customer due diligence, appropriate detection and reporting of suspicious activity and independent program testing.

While recognizing that all the components of an effective compliance program are important, FinCEN stresses the independence that the testing of a compliance program should have. A financial institution's leadership should ensure that the party testing the program (whether internal or external) is independent, qualified, unbiased and does not have conflicting business interests that may influence the outcome of the compliance program test. Safeguarding the integrity and independence of the compliance program testing enables an institution to locate and take appropriate corrective actions to address BSA/AML deficiencies.

Leadership and Staff Should Understand How Their BSA Reports are Used

Finally, leadership and staff at all levels in a financial institution should understand that they are not simply generating reports for the sake of compliance, but rather recognize the purpose that BSA reports serve and how the information is used. The reporting and the transparency that financial institutions provide under FinCEN's regulations result in some of the most important information available to law enforcement and others safeguarding the nation. It is used to confront serious threats, including terrorist organizations, rogue nations, weapons of mass destruction (WMD) proliferators, foreign corruption and, increasingly, some cyber related threats. The reporting that financial institutions provide also assists in the fight against transnational criminal organizations including those involved in drug trafficking and massive fraud schemes targeting the U.S. government, our businesses and our people.

The information may also help an institution protect itself and aid law enforcement in protecting the institution from bad actors, including insider threats, frauds and cyber-related threats such as spear phishing, account takeovers and distributed denial of service attacks, when such reports are filed.

Additionally, the very existence of BSA regulations has a deterrent effect on those who would abuse the financial system. The certainty of a Currency Transaction Report (CTR) filing and the mere possibility of a SAR filing force illicit actors to behave in ways that expose them to scrutiny and capture.

The reporting that financial institutions provide is used to:

1. Serve as tips to initiate investigations: BSA reports contribute critical information that is routinely analyzed, resulting in the identification of suspected criminal activity and the initiation of investigations. For instance, approximately 100 SAR review teams across the country bring together investigators and prosecutors from different governmental agencies to review reports related to their geographic area of responsibility and use the information therein to initiate criminal investigations, where appropriate.
2. Expand existing investigations: The reporting aids in expanding the scope of ongoing investigations by pointing to the identities of previously unknown subjects, exposing accounts and hidden financial relationships, or revealing other information such as common addresses or phone numbers that connect seemingly unrelated participants in a criminal or terrorist organization and, in some cases, even confirming the location of suspects. Nearly 11,000 federal, state and local law enforcement and regulatory users conduct roughly 30,000 searches per day of the reporting using FinCEN's information technology tool for making queries about known subjects.
3. Promote international information exchange: The Egmont Group has developed mechanisms for the rapid exchange of sensitive information between 146 Financial Intelligence Units (FIUs) around the world. In FY 2014, based on current trends, it is estimated that FinCEN will receive approximately 1,300 incoming Egmont requests from foreign FIUs seeking information derived from BSA reporting and make approximately 700 outgoing Egmont requests on behalf of U.S. law enforcement agencies seeking similar information from foreign FIUs.
4. Identify significant relationships, trends and patterns: BSA reports unmask the relationships between illicit actors and their financing networks, enabling law enforcement to target the underlying conduct of concern, and to use forfeiture and sanctions to disrupt their ability to operate and finance their illicit conduct. BSA reports also reveal trends and patterns on criminal, terrorist and other emerging threats that enable law enforcement to focus limited resources.

Understanding and communicating the context and the purpose of FinCEN's BSA/AML regime is as important to a financial institution's culture as understanding its underlying requirements, and financial institutions should consider including such information as part of their ongoing training requirement. Information on how BSA reports are used can be found on FinCEN's website and is routinely shared through numerous public-private training events involving FinCEN and its many law enforcement partners.

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at (800) 767-2825 or (703) 905-3591. Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial

Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

Part 2: SAR Filing Guidance

Systems to Identify and Report Suspicious Activity—Overview

Introduction. 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. Financial Institutions should recognize that the overall effectiveness of their SAR program is critical to the adequacy and effectiveness of the larger national system.

Within a bank's SAR program, 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. However, banks should establish effective policies, procedures, and processes to identify, evaluate, and report suspicious activity.

Background of Requirements. Banks, bank holding companies, and their subsidiaries are required by federal regulations 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).
- Is designed to evade the BSA or its implementing regulations.
- 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, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

Identifying Underlying Crime. Banks are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and certain other crimes above prescribed dollar thresholds. 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. Part III, section 35, of the SAR provides 20 different characteristics of suspicious activity. Although an "Other" category is available, the use of this category should be limited to situations that cannot be broadly identified within the 20 characteristics provided.

Safe Harbor. Federal law 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.

Overview of 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. These systems are discussed further in our Management Information Systems section of the manual.

Generally, effective suspicious activity monitoring and reporting systems include four key components as follows:

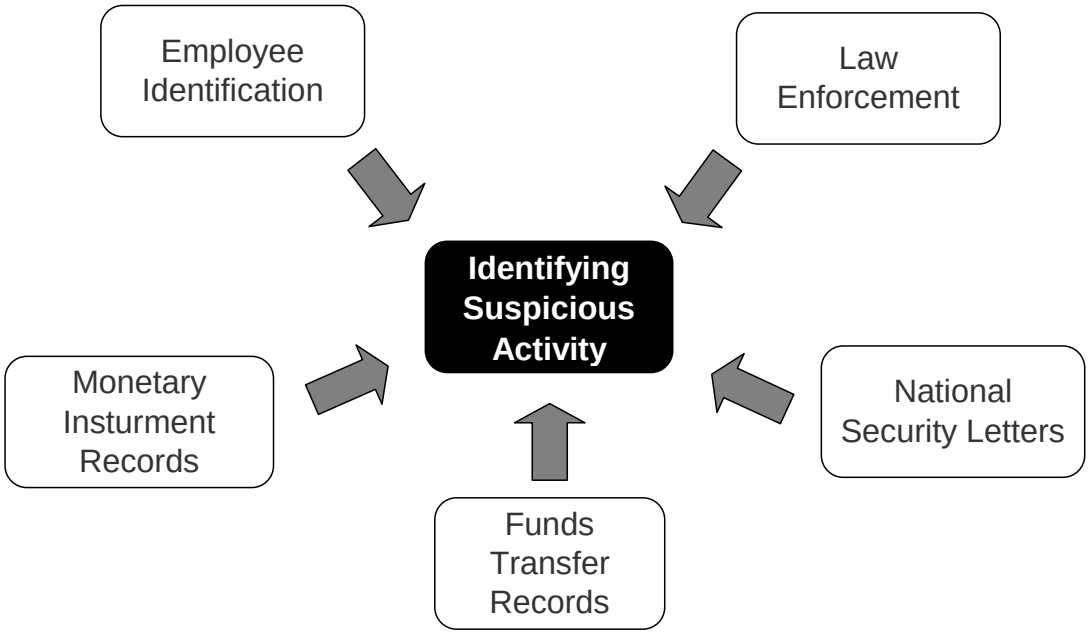
1. Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output).
2. Managing alerts.
3. SAR decision making.
4. SAR completion and filing.

These components 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.

These four components are present in banks of all sizes. However, the structure and formality of the components may vary. Larger banks will 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, and SAR completion and filing.

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 314(a) and 314(b) requests, 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.

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. 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.
- Information from credit bureaus.
- Financial records from financial institutions.

NSLs are highly confidential documents; for that reason, examiners will not review or sample specific NSLs.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 FBI field offices can be found at www.fbi.gov.

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.

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

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 will assist banks in evaluating if the unusual activity is considered suspicious. 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.

Managing Multiple Departments

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.

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 will be based on unique facts and circumstances, no single form of documentation is required when a bank decides not to file.

The decision to file a SAR is an inherently subjective judgment. Examiners will 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 by an examiner for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.

Ongoing SAR Filings

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 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 suggest that banks should report continuing suspicious activity by filing a report about every 90 days. This practice helps notify law enforcement of the continuing nature of the activity in aggregate. In addition, this practice will remind 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.

Escalation Process

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

While not a primary focus of this course, 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 SAR forms 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.

Timing of a SAR Filing

The SAR rules require that a SAR be filed 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.

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

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" will vary 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.

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.

SAR Quality

Banks are required to file SAR forms that are complete, thorough, and timely. Banks should include all known subject information on the SAR form. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR form, 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 form, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

By their nature, SAR narratives are subjective, and examiners will generally 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 form.

Board Notification

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 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.

SAR Retention

Banks must retain copies of SARs and supporting documentation for five years from the date of filing the SAR. 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.

Section 2: SAR Guidance on Elder Abuse

Introduction

On February 22, 2011, FinCEN issued FIN-2011-A003, which provides guidance in regards to filing SARs related to elder abuse. That guidance can be found at the following address and is listed below, as found in the guidance: https://www.fincen.gov/statutes_regs/guidance/html/fin-2011-a003.html.

Although this document was issued several years ago, it is still quite relevant to the everyday life of a bank.

FIN-2011-A003

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to assist the financial industry in reporting instances of financial exploitation of the elderly, a form of elder abuse. Financial institutions can play a key role in addressing elder financial exploitation due to the nature of the client relationship. Often, financial institutions are quick to suspect elder financial exploitation based on bank personnel familiarity with their elderly customers. The valuable role financial institutions can play in alerting appropriate authorities to suspected elder financial exploitation has received increased attention at the state level; this focus is consistent with an upward trend at the federal level in Suspicious Activity Reports (SARs) describing instances of suspected elder financial exploitation. Analysis of SARs reporting elder financial exploitation can provide critical information about specific frauds and potential trends, and can highlight abuses perpetrated against the elderly.

This advisory contains examples of "red flags" based on activity identified by various state and federal agencies and provides a common narrative term that will assist law enforcement in better identifying suspected cases of financial exploitation of the elderly reported in SARs.

Older Americans hold a high concentration of wealth as compared to the general population. In the instances where elderly individuals experience declining cognitive or physical abilities, they may find themselves more reliant on specific individuals for their physical well-being, financial management, and social interaction. While anyone can be a victim of a financial crime such as identity theft, embezzlement, and fraudulent schemes, certain elderly individuals may be particularly vulnerable.

Potential Indicators of Elder Financial Exploitation

The following red flags could indicate the existence of elder financial exploitation. This list of red flags identifies only *possible* signs of illicit activity. Financial institutions should evaluate indicators of potential financial exploitation in combination with other red flags and expected transaction activity being conducted by or on behalf of the elder. Additional investigation and analysis may be necessary to determine if the activity is suspicious.

Financial institutions may become aware of persons or entities perpetrating illicit activity against the elderly through monitoring transaction activity that is not consistent with expected behavior. In addition, financial institutions may become aware of such scams through their direct interactions with elderly customers who are being financially exploited. In many cases, branch personnel familiarity with specific victim customers may lead to identification of anomalous activity that could alert bank personnel to initiate a review of the customer activity.

- Erratic or unusual banking transactions, or changes in banking patterns:
    - Frequent large withdrawals, including daily maximum currency withdrawals from an ATM;
    - Sudden Non-Sufficient Fund activity;
    - Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds;
    - Debit transactions that are inconsistent for the elder;
    - Uncharacteristic attempts to wire large sums of money;
    - Closing of CDs or accounts without regard to penalties.
- Interactions with customers or caregivers:
    - A caregiver or other individual shows excessive interest in the elder's finances or assets, does not allow the elder to speak for himself, or is reluctant to leave the elder's side during conversations;
    - The elder shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker;
    - The financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her;
    - A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation;
    - The customer moves away from existing relationships and toward new associations with other "friends" or strangers;
    - The elderly individual's financial management changes suddenly, such as through a change of power of attorney to a different family member or a new individual;
    - The elderly customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

Suspicious Activity Reporting

SARs continue to be a valuable avenue for financial institutions to report elder financial exploitation. Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Part 103 (future 31 CFR Chapter X), if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should then file a Suspicious Activity Report.

In order to assist law enforcement in its effort to target instances of financial exploitation of the elderly, FinCEN requests that financial institutions select the appropriate characterization of suspicious activity in the Suspicious Activity Information section of the SAR form and include the term "elder financial exploitation" in the narrative portion of all relevant SARs filed. The narrative should also include an explanation of why the institution knows, suspects, or has reason to suspect that the activity is suspicious. It is important to note that the potential victim

of elder financial exploitation *should not be reported as the subject* of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

Elder abuse, including financial exploitation, is generally reported and investigated at the local level, with Adult Protective Services, District Attorney's offices, sheriff's offices, and police departments taking key roles. We emphasize that filers should continue to report all forms of elder abuse according to institutional policies and the requirements of state and local laws and regulations, where applicable. Financial institutions may wish to consider how their AML programs can complement their policies on reporting elder financial exploitation at the local and state level.

Financial institutions with questions or comments regarding this Advisory should contact FinCEN's Regulatory Helpline at 800-949-2732.

Section 3: SAR Guidance on Marijuana Businesses

Marijuana Businesses

On February 14, 2014, FinCEN issued guidance (FIN-2014-G001) specific to filing SARs related to marijuana-related businesses. FinCEN's guidance can be found at the following address and is listed below as found on their website:

https://www.fincen.gov/statutes_regs/guidance/html/FIN-2014-G001.html

In addition to this guidance, the Minneapolis branch of the Federal Reserve issued guidance on June 16, 2015 to help clarify their expectations for member banks. While this guidance is specific to banks regulated by the Minneapolis branch of the Federal Reserve, this guidance can be used as a best practice by any financial institution. The full guidance can be found at the following web address and is listed below as found on the website:

https://www.minneapolisfed.org/publications/banking-in-the-ninth/bsa-expectations-for-marijuana-related-businesses

FIN-2014-G001

The Financial Crimes Enforcement Network ("FinCEN") is issuing guidance to clarify Bank Secrecy Act ("BSA") expectations for financial institutions seeking to provide services to marijuana-related businesses. FinCEN is issuing this guidance in light of recent state initiatives to legalize certain marijuana-related activity and related guidance by the U.S. Department of Justice ("DOJ") concerning marijuana-related enforcement priorities. This FinCEN guidance clarifies how financial institutions can provide services to marijuana-related businesses consistent with their BSA obligations, and aligns the information provided by financial institutions in BSA reports with federal and state law enforcement priorities. This FinCEN guidance should enhance the availability of financial services for, and the financial transparency of, marijuana-related businesses.

Marijuana Laws and Law Enforcement Priorities

The Controlled Substances Act ("CSA") makes it illegal under federal law to manufacture, distribute, or dispense marijuana. Many states impose and enforce similar prohibitions. Notwithstanding the federal ban, as of the date of this guidance, 20 states and the District of Columbia have legalized certain marijuana-related activity. In light of these developments, U.S. Department of Justice Deputy Attorney General James M. Cole issued a memorandum (the "Cole Memo") to all United States Attorneys providing updated guidance to federal prosecutors concerning marijuana enforcement under the CSA. The Cole Memo guidance applies to all of DOJ's federal enforcement activity, including civil enforcement and criminal investigations and prosecutions, concerning marijuana in all states.

The Cole Memo reiterates Congress's determination that marijuana is a dangerous drug and that the illegal distribution and sale of marijuana is a serious crime that provides a significant source of revenue to large-scale criminal enterprises, gangs, and cartels. The Cole Memo notes that DOJ is committed to enforcement of the CSA consistent with those determinations. It also notes that DOJ is committed to using its investigative and prosecutorial resources to address the most significant threats in the most effective, consistent, and rational way. In furtherance of

those objectives, the Cole Memo provides guidance to DOJ attorneys and law enforcement to focus their enforcement resources on persons or organizations whose conduct interferes with any one or more of the following important priorities (the "Cole Memo priorities"):

- Preventing the distribution of marijuana to minors;
- Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels;
- Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
- Preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
- Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
- Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
- Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on public lands; and
- Preventing marijuana possession or use on federal property.

Concurrently with this FinCEN guidance, Deputy Attorney General Cole is issuing supplemental guidance directing that prosecutors also consider these enforcement priorities with respect to federal money laundering, unlicensed money transmitter, and BSA offenses predicated on marijuana-related violations of the CSA.

Providing Financial Services to Marijuana-Related Businesses

This FinCEN guidance clarifies how financial institutions can provide services to marijuana-related businesses consistent with their BSA obligations. In general, the decision to open, close, or refuse any particular account or relationship should be made by each financial institution based on a number of factors specific to that institution. These factors may include its particular business objectives, an evaluation of the risks associated with offering a particular product or service, and its capacity to manage those risks effectively. Thorough customer due diligence is a critical aspect of making this assessment.

In assessing the risk of providing services to a marijuana-related business, a financial institution should conduct customer due diligence that includes: (i) verifying with the appropriate state authorities whether the business is duly licensed and registered; (ii) reviewing the license application (and related documentation) submitted by the business for obtaining a state license to operate its marijuana-related business; (iii) requesting from state licensing and enforcement authorities available information about the business and related parties; (iv) developing an understanding of the normal and expected activity for the business, including the types of products to be sold and the type of customers to be served (e.g., medical versus recreational customers); (v) ongoing monitoring of publicly available sources for adverse information about the business and related parties; (vi) ongoing monitoring for suspicious activity, including for any of the red flags described in this guidance; and (vii) refreshing information obtained as part of customer due diligence on a periodic basis and commensurate with the risk. With respect to information regarding state licensure obtained in connection with

such customer due diligence, a financial institution may reasonably rely on the accuracy of information provided by state licensing authorities, where states make such information available.

As part of its customer due diligence, a financial institution should consider whether a marijuana-related business implicates one of the Cole Memo priorities or violates state law. This is a particularly important factor for a financial institution to consider when assessing the risk of providing financial services to a marijuana-related business. Considering this factor also enables the financial institution to provide information in BSA reports pertinent to law enforcement's priorities. A financial institution that decides to provide financial services to a marijuana-related business would be required to file suspicious activity reports ("SARs") as described below.

Filing Suspicious Activity Reports on Marijuana-Related Businesses

The obligation to file a SAR is unaffected by any state law that legalizes marijuana-related activity. A financial institution is required to file a SAR if, consistent with FinCEN regulations, the financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution: (i) involves funds derived from illegal activity or is an attempt to disguise funds derived from illegal activity; (ii) is designed to evade regulations promulgated under the BSA, or (iii) lacks a business or apparent lawful purpose. Because federal law prohibits the distribution and sale of marijuana, financial transactions involving a marijuana-related business would generally involve funds derived from illegal activity. Therefore, a financial institution is required to file a SAR on activity involving a marijuana-related business (including those duly licensed under state law), in accordance with this guidance and FinCEN's suspicious activity reporting requirements and related thresholds.

One of the BSA's purposes is to require financial institutions to file reports that are highly useful in criminal investigations and proceedings. The guidance below furthers this objective by assisting financial institutions in determining how to file a SAR that facilitates law enforcement's access to information pertinent to a priority.

"Marijuana Limited" SAR Filings

A financial institution providing financial services to a marijuana-related business that it reasonably believes, based on its customer due diligence, does not implicate one of the Cole Memo priorities or violate state law should file a "Marijuana Limited" SAR. The content of this SAR should be limited to the following information: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) the fact that the filing institution is filing the SAR solely because the subject is engaged in a marijuana-related business; and (iv) the fact that no additional suspicious activity has been identified. Financial institutions should use the term "MARIJUANA LIMITED" in the narrative section.

A financial institution should follow FinCEN's existing guidance on the timing of filing continuing activity reports for the same activity initially reported on a "Marijuana Limited" SAR. The continuing activity report may contain the same limited content as the initial SAR, plus details about the amount of deposits, withdrawals, and transfers in the account since the last SAR. However, if, in the course of conducting customer due diligence (including ongoing monitoring for red flags), the financial institution detects changes in activity that potentially implicate one of the Cole Memo priorities or violate state law, the financial institution should file a "Marijuana Priority" SAR.

"Marijuana Priority" SAR Filings

A financial institution filing a SAR on a marijuana-related business that it reasonably believes, based on its customer due diligence, implicates one of the Cole Memo priorities or violates state law should file a "Marijuana Priority" SAR. The content of this SAR should include comprehensive detail in accordance with existing regulations and guidance. Details particularly relevant to law enforcement in this context include: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) details regarding the enforcement priorities the financial institution believes have been implicated; and (iv) dates, amounts, and other relevant details of financial transactions involved in the suspicious activity. Financial institutions should use the term "MARIJUANA PRIORITY" in the narrative section to help law enforcement distinguish these SARs.

"Marijuana Termination" SAR Filings

If a financial institution deems it necessary to terminate a relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, it should file a SAR and note in the narrative the basis for the termination. Financial institutions should use the term "MARIJUANA TERMINATION" in the narrative section. To the extent the financial institution becomes aware that the marijuana-related business seeks to move to a second financial institution, FinCEN urges the first institution to use Section 314(b) voluntary information sharing (if it qualifies) to alert the second financial institution of potential illegal activity. See Section 314(b) Fact Sheet for more information.

Red Flags to Distinguish Priority SARs

The following red flags indicate that a marijuana-related business may be engaged in activity that implicates one of the Cole Memo priorities or violates state law. These red flags indicate only possible signs of such activity, and also do not constitute an exhaustive list. It is thus important to view any red flag(s) in the context of other indicators and facts, such as the financial institution's knowledge about the underlying parties obtained through its customer due diligence. Further, the presence of any of these red flags in a given transaction or business arrangement may indicate a need for additional due diligence, which could include seeking information from other involved financial institutions under Section 314(b). These red flags are based primarily upon schemes and typologies described in SARs or identified by our law enforcement and regulatory partners, and may be updated in future guidance.

- A customer appears to be using a state-licensed marijuana-related business as a front or pretext to launder money derived from other criminal activity (i.e., not related to marijuana) or derived from marijuana-related activity not permitted under state law. Relevant indicia could include:
    - The business receives substantially more revenue than may reasonably be expected given the relevant limitations imposed by the state in which it operates.
    - The business receives substantially more revenue than its local competitors or than might be expected given the population demographics.
    - The business is depositing more cash than is commensurate with the amount of marijuana-related revenue it is reporting for federal and state tax purposes.
    - The business is unable to demonstrate that its revenue is derived exclusively from the sale of marijuana in compliance with state law, as opposed to revenue derived

from (i) the sale of other illicit drugs, (ii) the sale of marijuana not in compliance with state law, or (iii) other illegal activity.

  - The business makes cash deposits or withdrawals over a short period of time that are excessive relative to local competitors or the expected activity of the business.
  - Deposits apparently structured to avoid Currency Transaction Report ("CTR") requirements.
  - Rapid movement of funds, such as cash deposits followed by immediate cash withdrawals.
  - Deposits by third parties with no apparent connection to the accountholder.
  - Excessive commingling of funds with the personal account of the business's owner(s) or manager(s), or with accounts of seemingly unrelated businesses.
  - Individuals conducting transactions for the business appear to be acting on behalf of other, undisclosed parties of interest.
  - Financial statements provided by the business to the financial institution are inconsistent with actual account activity.
  - A surge in activity by third parties offering goods or services to marijuana-related businesses, such as equipment suppliers or shipping servicers.

- The business is unable to produce satisfactory documentation or evidence to demonstrate that it is duly licensed and operating consistently with state law.
- The business is unable to demonstrate the legitimate source of significant outside investments.
- A customer seeks to conceal or disguise involvement in marijuana-related business activity. For example, the customer may be using a business with a non-descript name (e.g., a "consulting," "holding," or "management" company) that purports to engage in commercial activity unrelated to marijuana, but is depositing cash that smells like marijuana.
- Review of publicly available sources and databases about the business, its owner(s), manager(s), or other related parties, reveal negative information, such as a criminal record, involvement in the illegal purchase or sale of drugs, violence, or other potential connections to illicit activity.
- The business, its owner(s), manager(s), or other related parties are, or have been, subject to an enforcement action by the state or local authorities responsible for administering or enforcing marijuana-related laws or regulations.
- A marijuana-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.
- The owner(s) or manager(s) of a marijuana-related business reside outside the state in which the business is located.
- A marijuana-related business is located on federal property or the marijuana sold by the business was grown on federal property.

- A marijuana-related business's proximity to a school is not compliant with state law.
- A marijuana-related business purporting to be a "non-profit" is engaged in commercial activity inconsistent with that classification, or is making excessive payments to its manager(s) or employee(s).

Currency Transaction Reports and Form 8300's

Financial institutions and other persons subject to FinCEN's regulations must report currency transactions in connection with marijuana-related businesses the same as they would in any other context, consistent with existing regulations and with the same thresholds that apply. For example, banks and money services businesses would need to file CTRs on the receipt or withdrawal by any person of more than $10,000 in cash per day. Similarly, any person or entity engaged in a non-financial trade or business would need to report transactions in which they receive more than $10,000 in cash and other monetary instruments for the purchase of goods or services on FinCEN Form 8300 (Report of Cash Payments Over $10,000 Received in a Trade or Business). A business engaged in marijuana-related activity may not be treated as a non-listed business under 31 C.F.R. § 1020.315(e)(8), and therefore, is not eligible for consideration for an exemption with respect to a bank's CTR obligations under 31 C.F.R. § 1020.315(b)(6).

*****

FinCEN's enforcement priorities in connection with this guidance will focus on matters of systemic or significant failures, and not isolated lapses in technical compliance. Financial institutions with questions about this guidance are encouraged to contact FinCEN's Resource Center at (800) 767-2825, where industry questions can be addressed and monitored for the purpose of providing any necessary additional guidance.

Minneapolis Federal Reserve Expectations for Marijuana-Related Businesses

Currently, 23 states and the District of Columbia, including three Ninth District states, have legalized certain marijuana-related activity. Bankers have asked for additional guidance on how to comply with Bank Secrecy Act (BSA) obligations related to customers engaged in the legalized marijuana industry. In this article, we give direction on providing financial services to marijuana-related businesses consistent with BSA obligations. We do that by briefly explaining guidance issued by law enforcement and the Financial Crimes Enforcement Network (FinCEN), defining marijuana-related businesses, and outlining due diligence requirements. We conclude with some recommendations for banks considering offering services to marijuana-related businesses.

Guidance

The Controlled Substances Act (CSA) makes it illegal under federal law to manufacture, distribute, or dispense marijuana. The U.S. Department of Justice (DOJ) issued a memorandum (Cole Memo) in 2013 providing guidance to federal prosecutors concerning marijuana enforcement under the CSA in light of conflicting state laws. The Cole Memo directs federal attorneys and law enforcement to focus enforcement resources on persons or organizations whose conduct interferes with eight identified priorities (Cole Memo priorities). The priorities

include preventing the distribution of marijuana to minors, preventing revenue from the sale of marijuana from going to criminal enterprises, and preventing the diversion of marijuana from states where it is legal to states where it is illegal.

On February 14, 2014, FinCEN released FIN-2014-G001: BSA Expectations Regarding Marijuana-Related Businesses (Guidance), providing direction on how financial service businesses can interact with marijuana-related businesses and comply with the Cole Memo. The Guidance allows banks to work with marijuana-related businesses that are operating in accordance with state laws and regulations. The Guidance also creates a three-tiered system for filing Suspicious Activity Reports (SARs) regarding marijuana-related businesses. Banks must use the following labels when filing SARs based on the bank's reasonable belief as to whether the business implicates one of the Cole Memo priorities: MARIJUANA LIMITED (business does not implicate a Cole Memo priority), MARIJUANA PRIORITY (business does implicate a Cole Memo priority), or MARIJUANA TERMINATION (bank has terminated the relationship). Further, banks must report any activity suspected to be outside of state regulations.

Defining Marijuana-Related Businesses and Due Diligence

Marijuana-related businesses are divided into two categories; directly related and indirectly related. Directly related businesses include growers and providers/dispensaries. Indirectly related businesses provide goods or services to growers/providers (e.g., a commercial landlord that leases property to marijuana-related businesses or a business that sells supplies to a provider). Banks must file SARs on activity involving marijuana-related businesses in accordance with this Guidance and existing FinCEN suspicious activity reporting requirements and thresholds. Banks must use the labels outlined above when filing for directly related businesses, but the SAR narrative labels are not required for indirectly related businesses.

Customer due diligence is a critical aspect of making a decision to open, close, or refuse any particular account or relationship. Key elements of the due diligence process for marijuana-related businesses include verifying the business license and developing an understanding of the expected activity for the customer, including expected cash flow. For direct marijuana-related businesses, banks should also obtain the state license authorizing the entity as a grower/provider. Banks must monitor account behavior on an ongoing basis to identify red flags indicating that a marijuana-related business may be engaged in activity that implicates one of the Cole Memo priorities or violates state law. The Guidance identifies 11 scenarios that could raise a red flag, including operating the business as a front for money laundering, being unable to produce state licensing documentation, seeking to conceal involvement in a marijuana-related business, or publicly available sources reveal negative information about the business or related parties.

Recommendations

Banks that choose to offer financial services to marijuana-related businesses may want to consider the following steps to ensure compliance with expectations of the Guidance:

- Remember that the DOJ reserves the right to enforce federal laws, including federal laws relating to marijuana, regardless of state law and the Cole Memo.[4]
- Ensure that the BSA Risk Assessment and applicable policies are updated, congruent with inherent risk, and reflect established practices.
- Perform appropriate due diligence.

  - Request all available business documents, including state licensing documentation.
  - Establish expected account activity.
  - Identify all related parties involved with the marijuana-related business consistent with Customer Identification Program requirements.
  - Perform a site visit.
- Perform enhanced ongoing monitoring for suspicious activity.
  - Obtain periodic financial statements and tax returns.
  - Monitor accounts for credit/debit and check transactions in addition to cash transactions.
  - Monitor publicly available sources for adverse information.
  - Perform periodic site visits.
- At a minimum, file SARs as required by the Guidance.
- Consider maintaining separate accounts for the various operations of the marijuana-related business for ease of monitoring.
  - Separate accounts could include payroll, ATM, expense, and tax payment accounts.

Banks should stay alert to changes in state laws regarding marijuana-related businesses. Banks may need to modify policies, procedures, and operations in light of such changes. Finally, all banks should be alert to the risk of inadvertently providing services to marijuana-related businesses. One way to avoid doing so is to question account names that include terms frequently associated with these businesses, such as "hydroponics."

Section 4: SAR Guidance for Human Trafficking and Human Smuggling

Overview

On September 11, 2014, FinCEN release *Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags*. This guidance was issued in FIN-2014-2008 and the information in this manual was taken directly from that guidance.

The intent of the guidance is to advise financial institutions on how to detect and report suspicious financial activity that may be related to human smuggling and/or human trafficking. Financial institutions, large and small, can play a critical role in identifying and reporting transactions related to these unlawful activities based on their observations when interacting with customers and their monitoring processes.

FinCEN, in collaboration with law enforcement agencies, non-governmental organizations and members of the financial industry, has identified financial indicators, or "red flags," that may indicate financial activity related to human smuggling or human trafficking. In addition to identifying red flags, this advisory provides common terms that financial institutions may use when reporting activity related to these crimes. The use of common terms will assist law enforcement in better identifying possible cases of human smuggling or human trafficking reported through Suspicious Activity Reports (SARs).

Human Smuggling

Acts or attempts to bring unauthorized aliens to or into the United States, transport them within the U.S., harbor unlawful aliens, encourage entry of illegal aliens, or conspire to commit these violations, knowingly or in reckless disregard of illegal status.

Human Trafficking

The act of recruiting, harboring, transporting, providing or obtaining a person for forced labor or commercial sex acts through the use of force, fraud or coercion.

Difference Between Smuggling and Trafficking

Human Smuggling

(i) Involves persons choosing to immigrate illegally.

(ii) Is limited to illegal migration or the harboring of undocumented aliens.

(iii) Involves foreign nationals.

(iv) The crime involves an illegal border crossing or the harboring of someone that illegally crossed the border.

Human Trafficking

(i) Involves the use of force or coercion and the exploitation of victims.

(ii) Includes, but is not limited to, involuntary servitude, forced labor, debt bondage, peonage and sexual exploitation.

(iii) Anyone can be a victim regardless of origin, sex, age or legal status.

(iv) There is no need for a person to cross a border to be trafficked; individuals can be trafficked within the borders of a country.

Understanding How Smuggling and Trafficking Work

There are a number of identifiable stages involved in human smuggling and in human trafficking during which traffickers may need to interact with the financial system. This advisory includes below a brief description of these stages to provide financial institutions with the necessary context to appropriately identify potential human smuggling and/or human trafficking-related transactions. Financial indicators, including those described in Appendices A and B, may reflect transactions associated with actions that facilitate one or more of the stages of human smuggling and/or human trafficking.

How Human Smuggling Works

Stages of Human Smuggling generally include:

Solicitation: A potential migrant may seek the services of a local facilitator/smuggler. Local facilitators/smugglers are often part of a larger smuggling network that works to bring migrants across a country border. In the United States, illegal migrants often originate from Mexico and Central America, but they may originate from anywhere in the world.

Transportation: Migrants may be smuggled through a number of different routes and transportation modes to avoid detection. The person may be transported by air, sea and/or land over an international border.

Payment: Payment to smugglers or to smuggling networks are generally conducted in one of three ways.

1. *Pay In Advance:* The migrant or the migrant's relatives provide full payment to the smuggler before traveling. This method of payment is often used by relatives of unaccompanied minors for their migration.

2. *Partial Payment:* A portion of the smuggling fees is paid prior to departure, with the remaining due upon arrival; final payment is often made by relatives of the migrant in the United States.

3. *On Arrival:* After the migrant is successfully smuggled, the migrant's relatives pay the full fee to the smuggler. This method of payment is often used by relatives of unaccompanied minors for their migration.

How Human Trafficking Works

Stages of Human Trafficking generally include:

Recruitment or Abduction: Traffickers obtain their victims through deception or force. For instance, traffickers may recruit victims through the use of kidnapping, false marriages, or advertisements offering employment or study abroad. Individuals from countries and geographic areas that have been affected by economic hardship, armed conflicts or natural disasters are particularly vulnerable to these tactics.

Transportation: After being collected, victims are transported to locations where they are exploited or sold to other traffickers. Victims may originate from abroad or within the United States and may be transported by air, sea and/or land domestically or internationally.

Exploitation: During this stage, traffickers profit from exploiting victims through forced labor, sexual exploitation, involuntary participation in crimes or other activity. Businesses in the service and manual labor industries (e.g., massage parlors, restaurants, farms, construction companies, domestic services) have been frequently used to exploit trafficked individuals. In contrast to the one-time illicit proceeds of human smuggling, this final phase of human trafficking may generate ongoing criminal proceeds.

How to Identify Human Smuggling and Trafficking Transactions

To help identify and report transactions possibly associated with human smuggling and human trafficking, FinCEN has identified a number of red flags (see Appendices A and B) that financial institutions may consider incorporating into their monitoring programs. In applying these red flags, financial institutions are advised that no single transactional red flag is a clear indicator of human smuggling or trafficking-related activity. Accordingly, financial institutions should consider additional factors, such as a customer's expected financial activity, when determining whether transactions may be associated with human trafficking.

The red flags described in Appendices A and B may be associated with one or more of the stages of human smuggling or trafficking described above and may be considered by all financial institutions. Some red flags may be common to several types of financial institutions (e.g., banks, money transmitters, credit unions) while other red flags may be unique to a specific type of financial institution. Appendices A and B describe the human smuggling/trafficking stages and/or types of financial institutions most closely associated with each red flag.

In order to more effectively evaluate transactional activity, financial institutions may consider reviewing transactions at the relationship level rather than at the account level. Relationship level reviews allow financial institutions to analyze a customer's transactions across multiple accounts instead of reviewing transactions that are conducted solely through one account. This approach may also be applied when monitoring for any type of suspicious activity to offer financial institutions a more comprehensive perspective on the customer's behavior and activity.

Finally, direct interactions by branch or floor personnel with customers during the course of daily transactions can also alert financial institutions to human smuggling or trafficking-related activity. In many cases, smugglers and traffickers and/or their victims may hold accounts or receive services from financial institutions. Observations made by branch or floor personnel can

lead to the identification of anomalous activity that could alert a financial institution to initiate a review of a customer's transactions.

FinCEN Guidance to Financial Institutions

Due to some similarities with legitimate financial activities, financial institutions may consider evaluating indicators of potential human smuggling or trafficking activity in combination with other red flags and factors, such as expected transaction activity, before making determinations of suspiciousness. No one transaction or red flag by itself is a clear indicator of human smuggling or trafficking. Additionally, in making a determination of suspiciousness, financial institutions are encouraged to use previous FinCEN advisories and guidance as a reference when evaluating potential suspicious activity. For instance, in May 2014 FinCEN published an advisory on the use and structure of funnel accounts, one of the red flags identified in Appendices A and B of this advisory. Financial institutions may consider incorporating the guidance outlined in this advisory in a manner that is commensurate with their risk profile and business model.

In evaluating whether certain transactions are suspicious and/or related to human smuggling or trafficking, financial institutions are encouraged to share information with one another, as appropriate, under Section 314(b) of the USA PATRIOT Act. Section 314(b) establishes a voluntary information sharing mechanism allowing financial institutions to share information with one another regarding possible terrorist activity or money laundering and provides financial institutions with the benefit of a safe harbor from liability that might not otherwise exist with respect to the sharing of such information. Thus, suspected money laundering involving the proceeds of human smuggling or human trafficking activity could be shared amongst financial institutions under Section 314(b).

Suspicious Activity Reporting

SARs continue to be a valuable avenue for financial institutions to report suspected human smuggling or trafficking. Consistent with the standard for reporting suspicious activity as provided for in 31 CFR Chapter X, if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, the financial institution should file a Suspicious Activity Report.

To assist law enforcement in targeting instances of human smuggling and trafficking, FinCEN requests that financial institutions include one or both of the below key term(s) in the Narrative and the Suspicious Activity Information:

"ADVISORY HUMAN SMUGGLING" and/or "ADVISORY HUMAN TRAFFICKING"

Financial institutions should include one or both terms to the extent that financial institutions are able to distinguish between human smuggling and human trafficking. The narrative should also include an explanation of why the institution knows, suspects, or has reason to suspect that the activity is suspicious. It is important to note that a potential victim of human smuggling or trafficking should not be reported as the subject of the SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR.

Section 5: SAR Narrative Guidance

SAR Narratives

In the first quarter of 2008, the Philadelphia branch of the Federal Reserve provided member banks with guidance for writing effective SAR narratives. While this guidance is specific to the banks governed by this branch of the Federal Reserve, this guidance can be used as a best practice for any financial institution. The guidance can be found at the following web address and is provided below as found on the website: https://www.philadelphiafed.org/bank-resources/publications/src-insights/2008/first-quarter/q1si3_08

Guidance for Writing Effective SAR Narratives

by Jennifer Salutric, Enforcement Specialist

*Tell what happened, tell it well, tell it concisely...*William F. Buckley, Jr.

Since 1996, depository institutions-including banks, bank holding companies, and nonbank subsidiaries of bank holding companies-have been required to file Suspicious Activity Reports (SARs) with the Financial Crimes Enforcement Network (FinCEN) when they detect a known or suspected violation of federal law, a suspicious transaction related to money laundering activity, or a violation of the Bank Secrecy Act (BSA). Specifically, a SAR must be filed under the following circumstances:

- Criminal violations involving insider abuse in any dollar amount
- Criminal violations aggregating $5,000 or more where a suspect can be identified
- Criminal violations aggregating $25,000 or more, regardless of a potential suspect
- Transactions aggregating $5,000 or more that may involve potential money laundering or violations of BSA or where the transaction has no business or apparent lawful purpose

The information contained in filings provides SAR users (FinCEN, law enforcement, federal regulators, and intelligence agencies) with valuable data for investigating and combating money laundering, terrorism, terrorist financing, and other financial crimes and identifying patterns and emerging trends in suspicious and criminal activities. However, the increasing volume of SARs (the number filed by depository institutions soared from 62,388 in 1996 to 567,000 in 2006) presents a challenge for users who must review the reports but have limited resources to dedicate to that process. Therefore, it is imperative that depository institutions submit SARs that are complete, accurate, and timely so the users can extract the most useful information efficiently. Depository institutions can improve the utility of SARs by composing clear, concise, and thorough narratives in Part V of the SAR form, Suspicious Activity Information Explanation/Description.

Given the importance of the narrative, the purpose of this article is to provide guidance on how to write effective SAR narratives.[1] The process for writing the narrative can be divided into two steps: compiling the information and formatting the relevant information in a cohesive manner.

Compiling Information for the Narrative

To the fullest extent possible, the preparer of the SAR should gather all information necessary to answer the following five essential questions, which comprise the basis of the SAR narrative.

1. **Who** is conducting the suspicious activity? Fully describe and identify all suspects with respect to their occupation, position, or title within the business and the nature of the business. Explain the relationship amongst the suspects, and provide any other identification numbers, addresses, and aliases not reported elsewhere on the SAR form.
2. **What** instruments or mechanisms were used to facilitate the suspicious activity? Fully describe these instruments, which may include, but are not limited to, wire transfers, letters of credit, correspondent accounts, structuring, shell companies, bonds/notes, stocks, mutual funds, insurance policies, travelers checks, bank drafts, money orders, credit/debit cards, stored value cards, and/or digital currency business services.

   Preparers also should explain briefly and clearly **how** the suspicious activity was conducted, documenting the method used to initiate the transaction, such as the Internet, phone, mail, ATM, and couriers. When describing the flow of funds, include the source of funds and the use, destination, or beneficiary of the funds. Identify all account numbers at financial institutions affected by the suspicious activity and, if possible, the account numbers held at other financial institutions involved, along with the institutions' names and locations.
3. **When** did the suspicious activity take place? Record the date when the suspicious activity was first noticed and the timeframe in which it occurred. To better track the flow of funds, list the individual dates and the amounts of each transaction in chronological order rather than just the aggregate amount of all transactions.
4. **Where** did the suspicious activity occur? If multiple offices of a single institution were involved in the suspicious activity, provide the addresses of these locations. If the activity or transaction involved a foreign jurisdiction, provide the name of the jurisdiction and the name and address of any financial institutions involved, with any corresponding account numbers, if possible.
5. **Why** is the activity considered suspicious? Explain why the activity is unusual for the customer, considering the types of products and services offered by the institution and the typical activities of similar customers. The following is a sample, not a comprehensive list, of common patterns of suspicious activity:
   - A lack of evidence of legitimate business activity, or any business operations at all, undertaken by many of the parties involved in the transactions
   - Transactions that are not commensurate with the stated business type and/or that are unusual and unexpected in comparison with the volumes of similar businesses
   - Unusually large numbers and/or volumes of wire transfers and/or repetitive wire transfer patterns
   - Unusually complex series of transactions indicative of layering activity involving multiple accounts, banks, parties, or jurisdictions
   - Bulk cash and monetary instrument transactions

- Transactions seemingly designed or attempting to avoid reporting and recordkeeping requirements
- Transactions being conducted in bursts of activities within a short period of time, especially in previously dormant accounts
- Beneficiaries maintaining accounts at foreign banks that have been subjects of previous SAR filings
- Parties and businesses that do not meet the standards of routinely initiated due diligence and anti-money laundering oversight programs

Formatting the Narrative

Once all the necessary information has been compiled, it must be transcribed into the SAR narrative in a succinct, comprehensive, and well-organized format. Do not insert tables or other pre-formatted templates in the narrative because the conversion process used by the IRS Detroit Computing Center does not convert them properly, and the information becomes indecipherable. Also, do not submit any supporting documentation with the SAR form, because such documents are not entered into the database, thus making any reference to them meaningless. If possible, perform a second review of the SAR to ensure accuracy and completeness. In particular, verify that the suspicious activity described in the narrative matches the activity indicated in Part III of the SAR form, Suspicious Activity Information.

The following outline may be used as a guide for composing a more effective SAR narrative.

I. Introduction

This section can include:

- A brief description of the institution filing the report and its primary business
- The purpose of the SAR, including a general description of the known or alleged violation or activity and a summary of the suspicious patterns that initiated the SAR
- The date of and reason for any SARs previously filed on the suspect or related suspects
- Whether the SAR is associated with the Office of Foreign Assets Control's (OFAC) sanctioned countries or Specially Designated Nationals and Blocked Persons or other government lists for individuals or organizations

II. Body

This section should provide, in chronological order, all pertinent information supporting why the SAR was filed, including the following:

- The key components of the answers to the following questions: *Who is conducting the suspicious activity? What instruments were used to facilitate the suspicious activity? When, where, and how did the suspicious activity occur? Why is the activity considered suspicious?*

- Any other information not recorded elsewhere on the SAR that could aid investigations
- Any factual observations or incriminating statements made by the suspect

III. Conclusion

The final section can summarize the report and might also include:

- Information about any follow-up actions conducted by the depository institution
- Names and telephone numbers of other contacts at the depository institution, if different from the point of contact indicated in Part IV of the SAR form, Contact for Assistance
- Any additional information or documentation that may be made available to law enforcement
- Names of any law enforcement personnel investigating the complaint who are not already identified in another section of the SAR

The guidance presented above provides depository institutions with a methodology for preparing quality SAR narratives. As stated earlier, incomplete and insufficient SAR narratives waste the valuable time of law enforcement and investigatory resources and hinder investigations. By writing concise, comprehensive, and well-organized narratives, depository institutions provide SAR users with the crucial information they need to conduct investigations into financial crimes and to identify emerging trends and threats.

In addition, improving the quality of SARs can benefit a depository institution directly. By analyzing their SARs internally, a depository institution may also be able to identify any potential operational weakness and better assess its risk profile. Preparing accurate and timely SARs is required by law and is a key requirement of an institution's BSA/AML program. During a BSA/AML examination, examination staff will assess the policies, procedures, processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting SARs. Consequently, the systemic failure to file SARs, systemic filing of incomplete or inaccurate SARs, or failure to maintain an adequate BSA/AML compliance program could result in supervisory action against the institution; its board of directors, officers, employees, or agents; or other institution-affiliated parties.

This article focused on just one aspect of the SAR report, the narrative. For additional information regarding SARs, please refer to the following documents produced by FinCEN: *SAR Activity Review, Trends, Tips, and Issues* and *Suspicious Activity Reporting Guidance*, which are both available online, and *Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting*, which is also available online.

Prepared Remarks of FinCEN Director Jennifer Shasky Calvery, delivered at the FSSCC-FBIIC joint meeting

On December 9, 2015, FinCEN Director Jennifer Shasky Calvery spoke at the FSSCC-FBIIC joint meeting. The following is a portion of her prepared remarks that appear extremely relevant to BSA Officers:

"A key component to guarding against cyber threats is information sharing within the institution itself. If I could leave each of you with one piece of advice, which I have been discussing since FinCEN issued its "Culture of Compliance" Advisory in August 2014, it would be to share information across the business lines of your institution. As noted in the Advisory, there is information in various departments within a financial institution that may be useful and should be shared. For example, information developed by those in your institution that work to combat cyber threats could also assist your institution in complying with its BSA/AML obligations and assisting law enforcement to combat those threats. So my hope would be that after you leave here today, you will seek out your institution's AML officer to discuss how you can share information with each other that will ultimately benefit your entire institution through enhanced information sharing with law enforcement.

FinCEN also is strongly encouraging financial institutions to leverage their internal information technology resources to include cyber-derived information (such as IP addresses or bitcoin wallet addresses) in suspicious activity reports; to file these SARs voluntarily on cyber-attacks, and, to participate in voluntary information sharing with other financial institutions under the safe harbor granted in Section 314(b) of the USA PATRIOT Act.

I would like to underscore this point regarding IP address information: Less than two percent of SARs filed contain IP information. This information is incredibly important to the FinCEN analysts and law enforcement investigators working to combat cyber-crimes.

Information sharing between FinCEN and the financial industry is critically important as well. While FinCEN is constrained from sharing certain SAR information with financial institutions, such as the filing institution or the customer and account information, we can provide "research, analytical and informational services to financial institutions … to assist … in the detection and prevention of terrorism, organized crime, money laundering, and other financial crimes." This allows FinCEN to share attribution information derived from SARs and subjected to analysis that does not otherwise reveal sensitive customer or filer information. We are currently in the process of exploring ways to share cyber threat information derived from BSA reports with U.S. financial institutions in efforts to prevent and guard against cyber-attacks and cyber-enabled crime and protect the critical infrastructure."

Section 6: FinCEN Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime

Overview

Cyber Security is one of the hottest topics in banking right now. Scams, cyber-attacks, and malicious malware are among the top concerns of federal banking regulators. Cybercriminals target the financial system to defraud financial institutions and their customers and to further other illegal activities. Financial institutions can play an important role in protecting the U.S. financial system from these threats.

On October 25, 2016, the Financial Crimes Enforcement Network (FinCEN) issued an advisory to financial institutions on cyber-events and cyber-enabled crime. In addition to the advisory, FinCEN issued Frequently Asked Questions (FAQs) regarding the reporting of cyber-events, cyber-enabled crime, and cyber-related information through Suspicious Activity Reports.

This following portions of the manual include guidance from FinCEN:

- Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime
- Frequently Asked Questions (FAQs)

The original advisory and frequently questions can be found on FinCEN's website at: www.fincen.gov.

Advisory on Cyber-Events and Cyber-Enabled Crime

Cybercriminals target the financial system to defraud financial institutions and their customers and to further other illegal activities. Financial institutions can play an important role in protecting the U.S. financial system from these threats.

This Advisory should be shared with:

- Cybersecurity units
- Network administrators
- Risk departments
- Fraud prevention units
- BSA/AML management
- AML intelligence units
- AML analysts/investigators

The proliferation of cyber-events and cyber-enabled crime represents a significant threat to consumers and the U.S. financial system. The Financial Crimes Enforcement Network (FinCEN) issues this advisory to assist financial institutions in understanding their Bank

Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime. This advisory also highlights how BSA reporting helps U.S. authorities combat cyber-events and cyber-enabled crime.

Through this advisory FinCEN advises financial institutions on:

1. Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs);
2. Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs;
3. Collaborating between BSA/Anti-Money Laundering (AML) units and in-house cybersecurity units to identify suspicious activity; and
4. Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime.

For the purpose of this advisory:

- Cyber-Event: An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information.
- Cyber-Enabled Crime: Illegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.
- Cyber-Related Information: Information that describes technical details of electronic activity and behavior, such as IP addresses, timestamps, and Indicators of Compromise (IOCs). Cyber-related information also includes, but is not limited to, data regarding the digital footprint of individuals and their behavior.

Background

The size, reach, speed, and accessibility of the U.S. financial system make financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and state actors. These actors target financial institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information; defraud financial institutions and their customers; or disrupt business functions. Financial institutions can play an important role in safeguarding customers and the financial system from these threats through timely and thorough reporting of cyber-events and cyber-related information in SARs.

Value of BSA Reporting in Combating Cybercriminals and Cyber-Enabled Crime

FinCEN and law enforcement regularly use information financial institutions report under the BSA to initiate investigations, identify criminals, and disrupt and dismantle criminal networks. The cyber-related information that financial institutions include in this reporting is a valuable source of investigatory leads. Law enforcement has been able to use cyber-related

information reported—such as IP addresses with timestamps, cyber-event data, and virtual-wallet information—to track criminals, identify victims, and trace illicit funds.

For example, BSA reporting by more than 20 financial institutions—on transactions related to cyber-enabled crimes—played an important role in the investigation of an internet-based company, its co-founders, and other collaborators. This company acted as an unregistered online money-transmitting business and offered digital currency services specifically designed to provide anonymity to facilitate international crime and money laundering. Criminals used this company to conduct over $6 billion in illicit transactions involving proceeds from cyber-attacks, credit card fraud, child pornography, Ponzi schemes, identity theft, and trafficking in narcotics and other contraband.

Regulatory Expectations

This advisory does not change existing BSA requirements or other regulatory obligations for financial institutions. Financial institutions should continue to follow federal and state requirements and guidance on cyber-related reporting and compliance obligations.

Financial institutions should also note that filing a SAR does not relieve financial institutions from any other applicable requirements to timely notify appropriate regulatory agencies of events concerning critical systems and information or of disruptions in their ability to operate. In addition, the recently enacted Cybersecurity Act of 2015, also known as the Cybersecurity Information Sharing Act (CISA), does not change any SAR-reporting requirements under the BSA, SAR confidentiality rules, or the safe harbor protections under section 314 of the USA PATRIOT Act.

Guidance to U.S. Financial Institutions

The following guidance explains how BSA regulations and requirements apply to cyber-events, cyber-enabled crime, and cyber-related information.

I. SAR Reporting of Cyber-Events

Cyber-events targeting financial institutions often constitute criminal activity and can serve as means to commit a wide range of further criminal activity. For instance, criminals may seek to obtain unauthorized electronic access to electronic systems, services, resources, or information to conduct unauthorized transactions. Cyber-events can target or affect funds directly—such as in cases of fraud, identity/credential theft, and misappropriation of funds. Similarly, cyber-events can generate illicit proceeds—such as in cases of ransomware attacks and the sale of stolen proprietary information and credit card numbers.

<u>Mandatory SAR reporting of cyber-events</u>

A financial institution is required to report a suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets. If a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or

series of transactions. Cyber-events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities.

In determining whether a cyber-event should be reported, a financial institution should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event.

Financial institutions should also be familiar with any other cyber-related SAR-filing obligations required by their functional regulator. For instance, the Office of the Comptroller of the Currency (OCC) requires national banks to file SARs to report unauthorized electronic intrusions. The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) issued guidance concerning the filing of SARs to report certain computer-related crimes.

The following examples illustrate situations in which SAR reporting of cyber-events is mandatory. These examples do not, however, describe all instances when cyber-events require the filing of a SAR.

Example 1: Through a malware intrusion (a type of cyber-event), cybercriminals gain access to a bank's systems and information. Following its detection, the bank determines the cyber-event put $500,000 of customer funds at risk, based on the systems and/or information targeted by the cyber-event. Accordingly, the bank reasonably suspects the intrusion was in part intended to enable the perpetrators to conduct unauthorized transactions using customers' funds.

The bank must file a SAR because it has reason to suspect the cybercriminals, through the malware-intrusion, intended to conduct or could have conducted unauthorized transactions aggregating or involving at least $5,000 in funds or assets. As explained in the next section, the bank should include all available information in the SAR relevant to the suspicious activity, including cyber-related information such as a description and signatures of the cyber-event, attack vectors, command-and-control nodes, etc.

Example 2: Through a cyber-event, cybercriminals gain access to a financial institution's systems/networks. The cyber-event exposes sensitive customer information such as account numbers, credit card numbers, balances, limits, scores, histories, online-banking credentials, passwords/PINs, challenge questions and answers, or other similar information useful or necessary to conduct, affect, or facilitate transactions.

By evaluating the cyber-event and the type of information sought by its perpetrators, the financial institution reasonably suspects the cyber-event may have targeted information for the purpose of conducting, facilitating, or affecting transactions aggregating to at least $5,000. For instance, the financial institution could reasonably suspect the cybercriminals intended to steal and sell the exposed sensitive customer information to other criminals for financial exploitation to include unauthorized transactions at the institution. As further described below, the targeted financial institution should file a SAR to report all relevant information, including cyber-related information and information pertaining to any related unauthorized transactions.

Examples 1 and 2 describe instances where a financial institution should file a SAR in response to a cyber-event. Although no actual transactions may have occurred in these examples, the circumstances of the cyber-events and the systems and information targeted could reasonably lead the financial institutions to suspect the events were intended to be part of an attempt to conduct, facilitate, or affect an unauthorized transaction or series of unauthorized transactions aggregating or involving at least $5,000 in funds or assets.

Example 3: A Money Services Business (MSB) knows or suspects a Distributed Denial of Service (DDoS) attack prevented or distracted its cybersecurity or other appropriate personnel from immediately detecting or stopping an unauthorized $2,000 wire transfer.

In this case, the financial institution should file a single SAR to report both the unauthorized wire transfer and the related DDoS attack. The financial institution should report the transaction because it was unauthorized and meets the filing threshold; and it should report the DDoS attack because the DDoS attack was perpetrated to conceal the unauthorized wire transfer.

Voluntary reporting of cyber-events

FinCEN encourages, but does not require, financial institutions to report egregious, significant, or damaging cyber-events and cyber-enabled crime when such events and crime do not otherwise require the filing of a SAR.

To illustrate, consider a DDoS attack that disrupts a financial institution's website and disables the institution's online banking services for a significant period of time. After mitigating and investigating the DDoS attack, the affected financial institution determines the attack was not intended to and could not have affected any transactions. Although a financial institution is not required to report such DDoS attack, FinCEN encourages the financial institution to consider filing a SAR because the attack caused online banking disruptions that were particularly damaging to the institution. SAR reporting of cyber-events, even those that may not meet mandatory SAR-filing requirements, is highly valuable in law enforcement investigations.

II. Including Cyber-Related Information in SAR Reporting

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available, including cyber-related information. Because everyday financial transactions increasingly rely on electronic systems and resources, illicit financial activity often has a digital footprint, which may correspond to illicit actors and their associates, their activity, and related suspicious transactions.

Thus, financial institutions should include available cyber-related information when reporting any suspicious activity, including those related to cyber events as well as those related to other activity, such as fraudulent wire transfers. Cyber-related information includes, but is not limited to, IP addresses with timestamps, virtual-wallet information, device identifiers, and cyber-event information. FinCEN also encourages the filing of all such cyber-related information when a financial institution files a voluntary SAR. For additional information on reporting cyber-related information in SARs, please refer to these Frequently Asked Questions (FAQs) available on FinCEN's website.

Reporting cyber-related information involving cyber-events

When filing a mandatory or voluntary SAR involving a cyber-event, financial institutions should provide complete and accurate information, including relevant facts in appropriate SAR fields, and information about the cyber-event in the narrative section of the SAR—in addition to any other related suspicious activity. As needed, financial institutions may also attach a comma separated value (CSV) file to SARs to report data, such as cyber-event data and transaction details, in tabular form. For example, to the extent available, SARs involving cyber-events should include:

- Description and magnitude of the event
- Known or suspected time, location, and characteristics or signatures of the event
- Indicators of compromise
- Relevant IP addresses and their timestamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

Financial institutions subject to large numbers of cyber-events may report them through a single cumulative SAR filing when such events are similar in nature. For instance, a financial institution may file one SAR to report several malware intrusions if these events share common characteristics and indicators such as the methodology used, the vulnerability exploited, and IP addresses involved.

FinCEN also encourages financial institutions to incorporate cyber-related information into their BSA/AML monitoring efforts and report relevant cyber-related information in SARs. In the event a financial institution's filing software is not yet capable of including certain relevant information such as cyber-related information, as clarified by FinCEN in May 2013, the institution should manually complete discrete SAR filings until it updates its software to allow the inclusion such information. Financial institutions can submit discrete SARs through FinCEN's BSA E-Filing System.

This advisory is not intended to, and does not, create any new obligation or expectation requiring financial institutions to collect cyber-related information as a matter of course.

III. Collaboration between BSA/AML and Cybersecurity Units

As the examples above illustrate, collaboration and ongoing communication among BSA/AML, cybersecurity, and other units will help financial institutions conduct a more comprehensive threat assessment and develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime. Accordingly, financial institutions are encouraged to internally share relevant information from across the organization including, as appropriate, with BSA/AML staff, cybersecurity personnel, fraud prevention teams, and other potentially affected units.

Information provided by cybersecurity units could reveal additional patterns of suspicious behavior and identify suspects not previously known to BSA/AML units. For instance, BSA/AML units can use cyber-related information, such as patterns and timing of cyber-events and transaction instructions coded into malware among other things, to (1) help identify suspicious activity and criminal actors and (2) develop a more comprehensive understanding of their BSA/AML risk exposure. Likewise, cybersecurity personnel can use information provided by BSA/AML units to help the institution guard against cyber-events and cyber-enabled crime. In addition, this type of internal cooperation provides for more comprehensive and complete SAR reporting and is consistent with the principles involved in establishing a strong culture of compliance.

IV. Sharing Cyber-Related Information between Financial Institutions

Financial institutions can work together to identify threats, vulnerabilities, and criminals. By sharing information with one another, financial institutions may gain a more comprehensive and accurate picture of possible threats, allowing for more precise decision making in risk mitigation strategies. FinCEN continues to encourage financial institutions to use all lawful means to guard against money laundering and terrorist activities presented through cyber-events and cyber-enabled crime.

To encourage information sharing, Section 314(b) of the USA PATRIOT Act extends a safe harbor from liability to financial institutions—after notifying FinCEN and satisfying certain other requirements—that voluntarily share information with one another for the purpose of identifying and, where appropriate, reporting potential money laundering or terrorist activities. Under Section 314(b), financial institutions may share information, including cyber-related information, regarding individuals, entities, organizations, and countries for the purposes of identifying and reporting money laundering and terrorist activities. Thus, financial institutions may receive 314(b) safe harbor protections when sharing cyber-related information for the above mentioned purposes.

Cyber-related information, such as information about specific malware signatures, IP addresses and device identifiers, and seemingly anonymous virtual currency addresses, for example, can help identify the individuals, entities, organizations, or countries involved or responsible for the cyber-event or cyber-enabled crime linked to money laundering or terrorist activities.

For Immediate Assistance, Contact Regulatory and Law Enforcement Agencies

Financial institutions needing immediate assistance in the event of a cyber-event or a cyber-enabled crime should contact appropriate regulatory and law enforcement agencies. Regulatory and law enforcement agencies can help affected financial institutions normalize systems and operations and, in some cases, reduce monetary losses. The U.S. Department of Homeland Security (DHS) published a fact sheet on obtaining threat and asset response assistance following a cyber incident. In addition, the U.S. Department of Justice published a guide outlining appropriate government agencies to contact in the event of computer hacking, fraud, and other internet-related crime.

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov, (800) 767-2825 (Option 9), or (703) 905-3591 (Option 9). Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

Frequently Asked Questions

The following Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs) were taken directly from FinCEN's website at www.fincen.gov.

FAQs

- The following is a non-exhaustive list of relevant cyber-related information and identifiers associated with suspicious transactions and cyber-events that should be reported as available:
- The Financial Crimes Enforcement Network (FinCEN) provides the following FAQs to supplement its advisory on cyber-events and cyber-enabled crime and assist financial institutions in reporting cyber-events and cyber-enabled crime through SARs.
- The following FAQs supersede those published in 2001 regarding computer intrusion.
- These new FAQs provide information and details not contained in the 2001 FAQs.

1. Q: What information should a financial institution include in SARs when reporting cyber-events and cyber-enabled crime? Financial institutions are required to file complete and accurate reports that incorporate all relevant information available, including cyber-related information.

While suspicious transactions may not always involve a cyber-event, relevant cyber-related information should still be included in SARs when available. For instance, financial institutions should include available Internet Protocol (IP) addresses and accompanying timestamps associated with fraudulent wire transfers being reported, even if a cyber-event was not involved in the suspicious activity.

Similarly, when suspicious transactions do involve cyber-events, a financial institution should include in SARs all relevant and available information regarding the suspicious transactions and the cyber-event—including the type, magnitude, and methodology of the cyber-event as well as signatures and facts on a network or system that indicate a cyber-event.

- Source and Destination Information:
    - IP address and port information with respective date timestamps in UTC
    - Uniform Resource Locator (URL) addresses
    - Attack vectors
    - Command-and-control nodes
- File Information:
    - Suspected malware filenames
    - MD5, SHA-1, or SHA-256 hash information
    - E-mail content
- Subject User Names:
    - E-mail addresses
    - Social media account/screen names
- System Modifications:
    - Registry Modifications
    - Indicators of Compromise (IOCs)
    - Common vulnerabilities and exposures (CVEs)3
- Involved Account Information:
    - Affected account information
    - Involved virtual currency accounts (case sensitive)

2. Q: How should a financial institution complete SARs when reporting cyber-events and cyber-enabled crime?

Financial institutions should follow FinCEN's existing guidance when submitting SARs related to cyber-events and cyber-enabled crime. Financial institutions should include relevant information in pertinent SAR fields as well as a description of the facts surrounding the cyber-event or cyber-enabled crime in the narrative section. Recognizing that cyber-events and cyber-enabled crime may involve event-specific cyber-related information, FinCEN requests filing institutions to be consistent and use widely used and accepted terminology.

Completing the SAR Form

Financial institutions should enter available cyber-related information and identifiers, identified in FAQ 1 above, in their designated SAR fields. For example, specific SAR fields are available for providing IP addresses (item 44), website/URL addresses (item 19a), and e-mail addresses (item 19).

Relevant information with no pre-designated SAR field should be included in the SAR narrative.

Completing the SAR Narrative

Financial institutions should document and provide in the SAR narrative a detailed description of the suspicious activity (e.g., transactions, cyber-events) being reported. In addition, as described in FAQ 1, filers should include in the SAR narrative descriptive cyber-related information as well as cyber-related identifiers for which there is no pre-designated SAR field.

Filers may also include information as an attachment to the SAR. For example, filers may include in a SAR attachment patterns of online activity and other data, which may be easier to read and use in tabular format. FinCEN's SAR accepts a single comma separated value (CSV) file as an attachment. Please note that attachments are considered part of the SAR and are not a substitute for the narrative itself.

3. Q: How should cyber-events and cyber-enabled crime be characterized in SARs?

Financial institutions should categorize the activity being reported by selecting all applicable characterization checkboxes contained in Part II of the SAR, such as "Unauthorized Electronic Intrusion" (item 35q) or "Account Takeover" (item 35a). For SAR filing purposes, when suspicious activity (e.g., wire fraud) is also cyber-enabled crime, financial institutions should characterize the suspicious activity using the available SAR checkboxes (e.g. "Wire Fraud" item 31j). If no existing checkbox adequately characterizes the activity, filers should identify the suspicious activity in the "Other" field (item 35z) by entering widely-used and accepted terminology. Filers can select more than one characterization checkbox.

4. Q: How does a financial institution report numerous cyber-events in SARs?

FinCEN recognizes that filing a SAR to report individual cyber-events may require significant time and resources and could detract from a financial institution's efforts to guard against more significant money laundering and cyber threats.

Accordingly, a financial institution may file a single cumulative SAR to report multiple cyber-events when they are too numerous to be reported individually and:

- are similar in nature and share common identifiers, such as those described in FAQ 1 above or
- are believed to be related, connected, or part of a larger scheme.

Financial institutions can also use cumulative SARs to report mandatory and voluntary reporting of cyber-events. Financial institutions should only use cumulative SARs when reporting cyber-events and not other types of suspicious activity, which must be reported following normal SAR filing procedures.

5. Q: Is a financial institution required to file SARs to report continuous scanning or probing of a financial institution's systems or network?

No. FinCEN recognizes that filing a SAR to report each time an institution's system or network is scanned or probed is impractical and could detract from a financial institution's efforts to guard against more significant money laundering and cyber threats. However, when filing a SAR on a reportable cyber-event, financial institutions may include information about the scanning and probing of their systems and networks if available and relevant. To the extent that a financial institution reports scanning and probing, it may do so using cumulative SARs when such activity is too numerous to be reported individually.

6. Q: Should a SAR be filed in instances where an otherwise reportable cyber-event is unsuccessful?

Yes. An otherwise reportable cyber-event should be reported regardless of whether it is considered unsuccessful. Rather, a financial institution is required to file a SAR to report any cyber-event if the institution knows, suspects, or has reason to suspect the cyber-event was intended to or could affect a transaction conducted or attempted by, at, or through the financial institution. See FinCEN's Advisory FIN-2016-A005 on Cyber-Events and Cyber-Enabled Crime.

7. Q: Does FinCEN now require financial institutions' BSA/AML units to have personnel/systems devoted to cybersecurity?

No. There are no new requirements or obligations for financial institutions. FinCEN's Advisory FIN-2016-A005 and these FAQs do not change existing BSA or other expectations or regulatory obligations. Financial institutions should continue to follow federal and state government agencies' and pertinent regulatory organizations' guidance and requirements on cyber-related reporting and compliance obligations. This guidance should not be interpreted in a manner inconsistent with guidance previously issued by FinCEN, U.S. government agencies, or other regulatory organizations.

8. Q: Are BSA/AML personnel now required to be knowledgeable on cybersecurity and cyber-events?

No. There are no new requirements or obligations for financial institutions. A BSA/AML unit may work and collaborate as necessary with its institution's cybersecurity personnel, to assist in their ability to adequately identify and report suspicious activity, including cyber-events and cyber-enabled crime.

9. Q: Can financial institutions use Section 314(b) of the USA PATRIOT Act to share cyber-event and cyber-enabled crime information with other financial institutions?

Yes. Under Section 314(b), participating financial institutions may exchange information, including cyber-related information, regarding individuals, entities, organizations, and countries to identify and report money laundering and terrorist activities. Section 314(b) of the USA

PATRIOT Act provides financial institutions with the ability to share information voluntarily with one another—after notifying FinCEN and satisfying certain other requirements—under a safe harbor, which offers protections from liability under certain circumstances. In addition, under Section 314(b) any type of participating financial institution, such as a bank, may share information with any other participating institution, such as a credit card operator or a money transmitter.

Sharing cyber-related information and information related to cyber-event and cyber-enabled crime may:

- Aid in identifying and stopping cyber-events and cyber-enabled crime potentially connected to money laundering and terrorist activities.
- Build a more comprehensive and accurate picture of cyber-events and cyber-enabled crime potentially connected to money laundering or terrorist activities.
- Alert contacted financial institutions about customers whose information or credentials may have been compromised.
- Facilitate the filing of more comprehensive and complete SARs than would otherwise may have been filed, in the absence of 314(b) information sharing.

FinCEN's Section 314(b) Fact Sheet provides further information about the 314(b) information sharing program and outlines additional benefits available to program participants.