Elements of a Sound

Bank Secrecy Act /

Anti-Money Laundering

Compliance Program

NOTE: This document is intended to outline steps you can take to ensure that your compliance program is adequate.

BANK SECRECY ACT (BSA)/ANTI-MONEY LAUNDERING (AML) COMPLIANCE PROGRAMS

INTRODUCTION

Given the importance of compliance with the anti-money laundering requirements to the protection of our financial system and our national security, MSBs that fail to comply with even the most basic requirements of the Bank Secrecy Act, such as registration with FinCEN if required, not only are subject to regulatory and law enforcement scrutiny, but also are likely to lose banking services that enable them to function.

Like other financial institutions subject to the Bank Secrecy Act, MSBs must assess the risks of their operations as a step in developing effective anti-money laundering programs. MSBs seeking to obtain or maintain account relationships with banking organizations should be prepared to provide information or explanation to their banking organizations about the risks associated with the services offered, the customer base, the markets served, and the locations of the money services business.

Department examiners will assess the adequacy of your AML compliance program to determine whether you have developed, administered, and maintained an effective program for compliance with the BSA and all of its implementing regulations. Review of the MSB's written policies, procedures, and processes is a first step in determining the overall adequacy of the BSA/AML compliance program. The document provides guidance and elements for designing an effective MSB compliance program. The degree to which elements should be implemented are dependent upon the MSB's risk profile.

ANTI-MONEY LAUNDERING COMPLIANCE PROGRAMS

Each MSB is required by law to have an effective anti-money laundering (AML) compliance program. An effective anti-money laundering program is one that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. The regulation requiring MSBs to develop and maintain an AML compliance program is contained in 31 CFR Chapter X 1022.210. **Each program must be commensurate with the risks posed by the location, size, nature and volume of the financial services provided by the MSB**. For example, a large money transmitter with a high volume of business located in large metro area is at higher risk than a small check casher with a low volume of business located in a rural area. Therefore, the large money transmitter would be expected to have a more complex AML compliance program, commensurate with its higher risk, than the smaller check casher, who is at lower risk of being used to facilitate money laundering.

An effective program is one designed to prevent the MSB from being used to facilitate money laundering. Each AML compliance program must be <u>in writing</u> and must:

- Incorporate policies, procedures and internal controls reasonably designed to assure compliance with the BSA;

- X Designate a compliance officer responsible for day-to-day compliance with the BSA and the compliance program;
- X Provide education and/or training of appropriate personnel; and
- X Provide for independent review to monitor and maintain an adequate program.

Establish Customer Relationships

Strict customer identification and verification polices and procedures can be an MSB's most effective weapon against money laundering. Requiring appropriate identification and verifying information in certain cases, and being alert to unusual or suspicious transactions can help an MSB deter and detect money laundering schemes. A customer identification and verification policy tailored to the operations of a particular business:

- X Helps detect suspicious activity in a timely manner.
- X Promotes compliance with all state and federal laws applicable to MSBs.
- X Promotes safe and sound business practices.
- X Minimizes the risk that the MSB will be used for illegal activities.
- X Reduces the risk of government seizure and forfeiture of funds associated with customer transactions (such as outstanding money orders/traveler's checks and outstanding money transfers) when the customer is involved in criminal activity.
- X Protects the reputation of the MSB.

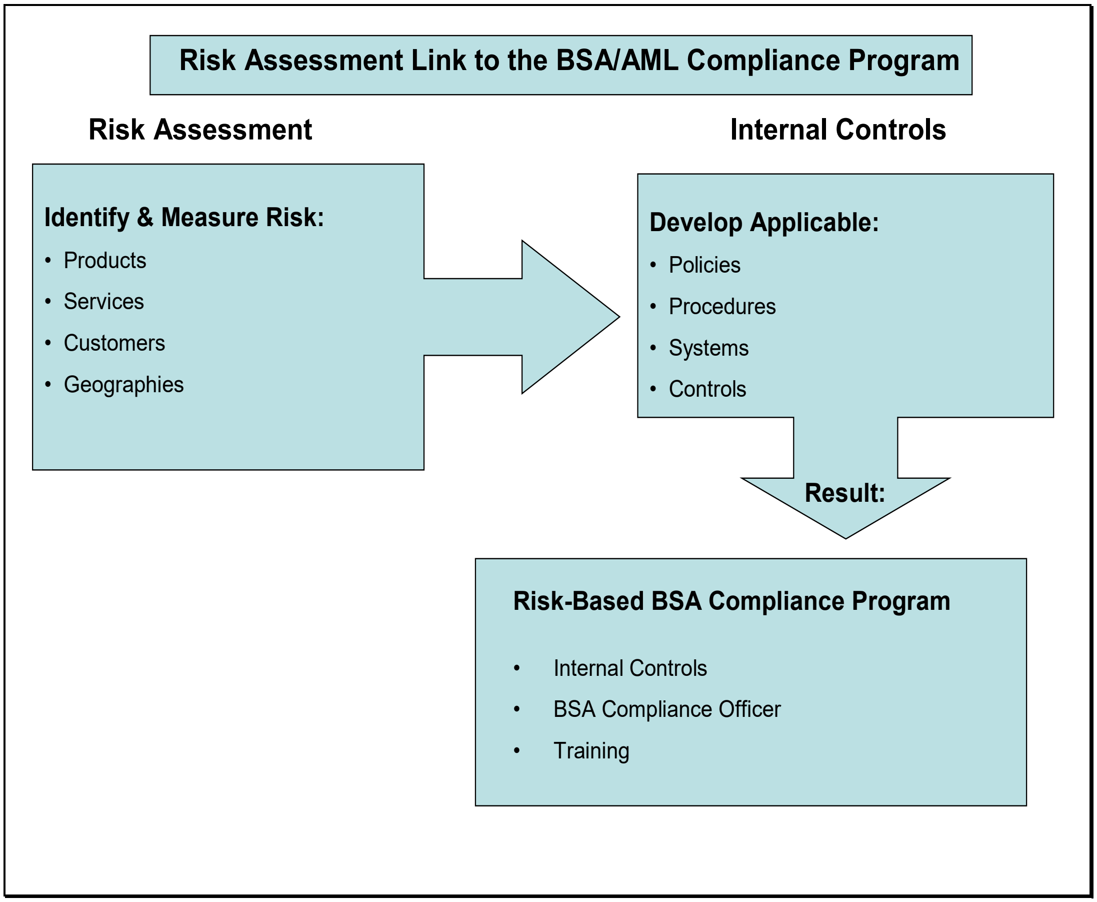
For further information refer to FinCEN's guides, interpretations, fact sheets, and advisories provided for MSBs at http://www.fincen.gov/financial_institutions/msb/msbrequirements.html for more information on money laundering prevention and BSA requirements.

Risk Assessment

As discussed earlier, each MSB must develop an AML Compliance Program that is commensurate with their level of risk. The MSB should not necessarily take any single indicator as determinative of the existence of lower or higher risk. The risk assessment process should weigh a number of factors, including the risk identification and measurement of products, services, customers, and geographic locations.

This risk assessment should assist the MSB in effectively managing the BSA/AML risk and therefore, is critical in the development of applicable internal controls, as required for the BSA/AML compliance program. A graphic description of the BSA/AML compliance program link to the risk assessment process is provided on the following page ("Risk Assessment Link to the BSA/AML Compliance Program").

An effective BSA/AML compliance program controls risks that may be associated with the MSB's unique products, services, customers, and geographic locations. As new products and services are introduced, existing products and services change, management's evaluation of the money laundering and terrorist financing should evolve. Furthermore, even without such changes, MSBs should periodically reassess their BSA/AML risks.



Internal Controls

Management is ultimately responsible for ensuring that the MSB maintains an effective BSA/AML internal control structure, including suspicious activity monitoring and reporting. MSB management should create a culture of compliance to ensure staff adherence to the BSA/AML policies, procedures, and processes. Internal controls are the MSB's policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks and complexity of the MSB's operations and lines of business.

Internal controls should:

- Identify operations (products, services, customers, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the risk profile; and provide for a BSA/AML compliance program tailored to manage risks.
- Inform the board of directors (if applicable) and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of Suspicious Activity Reports (SARs) filed.
- Identify a person or persons responsible for BSA/AML compliance.
- Provide for program continuity despite changes in management or employee composition or structure.

- Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance and provide for timely updates in response to changes in regulations.
- Implement customer identification and verification policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports including SARs and Currency Transaction Reports (CTRs), and FinCEN registration.
- Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.

The above list is not designed to be all-inclusive and should be tailored to reflect the MSB's risk profile.

Independent Testing (Audit)

Management should provide for independent review to monitor and maintain an adequate program. The scope and frequency of the review shall be commensurate with the risk of the financial services provided by the MSB. Such review may be conducted by an officer or employee of the MSB, as long as the reviewer is not the person designated as the BSA Compliance Officer.

<u>FinCEN's regulations do not require MSBs to retain outside auditors to conduct the independent test of an AML program</u>. This is especially important for small MSBs that may not have the ability to retain an outside auditing firm.

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 (MIS). The audit should be risk-based and evaluate the quality of risk management for all operations, departments, and subsidiaries. Risk-based audit programs will vary depending on the size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity, and use of technology. The testing should assist management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

Independent testing may include, but is not limited to the following:

- An evaluation of the overall integrity and effectiveness of the BSA/AML compliance program, including policies, procedures, and processes.

- A review of the risk assessment for reasonableness given the MSB's risk profile (products, services, customers, and geographic locations).

- Appropriate transaction testing to verify adherence to the BSA recordkeeping and reporting requirements.

- 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 MSB's policy.

The audit scope, procedures performed, transaction testing completed, and findings of the review should be documented. All audit / testing documentation and workpapers should be available for examiner review. Management should track audit deficiencies and document corrective actions.

BSA Compliance Officer

The MSB must designate a qualified employee to serve as the BSA compliance officer. The responsibilities of such person shall include assuring that:

1. The MSB properly files reports, and creates and retains records, in accordance with applicable requirements of this part;
2. The compliance program is updated as necessary to reflect current requirements of this part, and related guidance issued by the Department of the Treasury; and
3. The MSB provides appropriate training and education.

The BSA compliance officer should be fully knowledgeable of applicable BSA and all related regulations. The BSA compliance officer should also understand the MSB's products, services, customers, and geographic locations, and the potential money laundering and terrorist financing risks associated with those activities.

Training

MSBs must ensure that appropriate personnel are trained concerning their responsibilities under the BSA/AML compliance program, including training in the detection of suspicious transactions. Training should include regulatory requirements and the MSB's internal BSA/AML policies, procedures, and processes. In addition, an overview of the BSA/AML requirements should be given to new staff. Examples of money laundering activity and suspicious activity monitoring and reporting can and should be tailored to each individual audience.

MSBs should document their training programs. Training and testing materials, the dates of training sessions, etc. should be maintained and be available for examiner review.

Training should be ongoing and incorporate current developments and changes to the BSA and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems should also be covered during training. The program should reinforce the importance that management places on the MSB's compliance with the BSA and ensure that all employees understand their role in maintaining an effective BSA/AML compliance program.

TEMPLATES AND OTHER GUIDANCE

SUSPICIOUS ACTIVITY REPORT (SAR) QUALITY GUIDANCE

The following information is provided as guidance. Refer to FinCEN's website for further guidance at http://www.fincen.gov/forms/files/e-filing_SARMSBspecs.pdf.

Often SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in SAR forms also allows FinCEN to identify emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions and MSBs.

MSBs must file SAR forms that are complete, sufficient, and timely. Unfortunately, some SAR forms contain incomplete, incorrect, or disorganized narratives, making further analysis difficult, if not impossible. Some SAR forms are submitted with blank narratives. Because the SAR narrative serves as the only free text area for summarizing suspicious activity, the narrative section is "critical." The care with which the narrative is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood by law enforcement, and thus a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

The SAR form should include any information readily available to the filing entity at the time of the transaction. In general, a SAR narrative should identify the five essential elements of information (**who? what? when? where?** and **why?**) for the suspicious activity being reported. The method of operation (or **how?**) is also important and should be included in the narrative.

Who is conducting the suspicious activity?

While one section of the SAR form calls for specific suspect information, the narrative should be used to further describe the suspect or suspects, including occupation, position or title within the business, the nature of the suspect's business (or businesses), and any other information and identification numbers associated with the suspects.

What instruments or mechanisms are being used to facilitate the suspect transactions?

A list of instruments or mechanisms that may be used in suspicious activity includes, but is not limited to, funds transfers, structuring, traveler's checks, bank drafts, money orders, credit/debit cards, stored value cards, and digital currency business services. The SAR narrative should list the instruments or mechanisms used in the reported suspicious activity. If a SAR narrative summarizes the flow of funds, the narrative should always include the source of the funds (origination) and the use, destination, or beneficiary of the funds.

When did the suspicious activity take place?

If the activity takes place over a period of time, indicate the date when the suspicious activity was first noticed and describe the duration of the activity. Where possible, in order to better track the flow of funds, individual dates and amounts of transactions should be included in the narrative rather than only the aggregated amount.

Where did the suspicious activity take place?

The narrative should indicate if multiple offices of the MSB were involved in the suspicious activity and provide the addresses of those locations. The narrative should also specify if the suspected activity or transactions involves a foreign jurisdiction.

Why does the filer think the activity is suspicious?

The SAR should describe, as fully as possible, why the activity or transaction is unusual for the customer, considering the types of products and services offered, and drawing any applicable contrasts with the nature and normally expected activities of similar customers.

How did the suspicious activity occur?

The narrative should describe the “modus operandi” or the method of operation of the subject conducting the suspicious activity. In a concise, accurate, and logical manner, the narrative should describe how the suspect transaction or pattern of transactions was committed. For example, if what appears to be structuring of currency deposits is matched with outgoing funds transfers from the accounts, the SAR narrative should include information about both the structuring and outbound transfers (including dates, destinations, amounts, accounts, frequency, and beneficiaries of the funds transfers).

An MSB should not include any supporting documentation with a filed SAR nor use the terms “see attached” in the SAR narrative.

When SAR forms are received at the IRS Detroit Computing Center, only information that is in an explicit, narrative format is keypunched; thus, tables, spreadsheets or other attachments are not entered into the BSA-reporting database. MSBs should keep any supporting documentation in their records for five years so that this information is available to law enforcement upon request.

TRANSACTION TESTING TOOLS USED BY EXAMINERS

The following sections discuss transaction testing tools that may be utilized by examiners when they conduct an examination of your business. You may find many of these testing procedures beneficial for your own internal procedures.

Currency Transaction Reporting/Suspicious Currency Activity Reporting

If the MSB does not have preset filtering reports for currency transaction reporting and the identification of suspicious currency transactions the examiner may request a custom report. For example, a report could be generated with the following criteria: currency transactions of $7,000 or higher (in and out) for at time period to be determined by the examiner. The time period covered and the transaction amounts may be adjusted as determined by the examiner. The report should also capture:

- The Social Security number (SSN)/taxpayer identification number (TIN), or other customer identification number, if applicable.
- The date, amount, and account number of each transaction.
- The agent/branch or other applicable identifying information.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. The data can be sorted in a number of different criteria (e.g., by location, by agent, by SSN/TIN, etc.). Analysis of this information should enable the examiner to determine whether Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) have been appropriately filed.

Funds Transfer Monitoring

If the MSB does not have preset filtering reports for funds transfer recordkeeping and the identification of suspicious transactions the examiner may request a custom report. The examiner may ask the MSB to provide a report from its funds transfer systems that identifies all funds transfers (in and out) for a time period determined by the examiner. The report should also capture:

- The customer's full name, country of residence, SSN/TIN, and BSA/AML risk rating (if a risk rating system is utilized by the MSB).
- The date, amount, transaction type, and account number of each transaction.
- The originator's name, country, financial institution, and account number.
- The beneficiary's name, country, financial institution, and account number.

The MSB should provide a list of internal codes necessary to fully identify the account type, risk rating (if applicable), country, transaction type, account number, and any other codes on the electronic reports. The list should be sorted to identify those accounts that do not contain sufficient originator or beneficiary information. Missing information may indicate funds transfer monitoring deficiencies. A large number of transfers or those of high-dollar amounts to and from high-risk jurisdictions or involving parties that do not appear likely to be involved in such transactions may indicate the need for additional scrutiny.

OBJECTIVE

Assess the MSB's risk-based Office of Foreign Assets Control (OFAC) program to evaluate whether it is appropriate for the MSB's OFAC risk, taking into consideration its products, services, customers, transactions, and geographic locations.

PROCEDURES

1. Determine whether MSB management has developed policies, procedures, and processes based on their risk assessment to ensure compliance with OFAC laws and regulations.

2. Regarding the risk assessment, review the OFAC program. Consider the following:

   - The extent of, and method for, conducting OFAC searches of each relevant department/business line (e.g., money transmission, monetary instrument sales, check cashing) as the process may vary from one department or business line to another.
   - The extent of, and method for, conducting OFAC searches of customers.
   - How responsibility for OFAC is assigned.
   - Timeliness of obtaining and updating OFAC lists or filtering criteria.
   - The appropriateness of the filtering criteria used to reasonably identify OFAC matches (e.g., the extent to which the filtering/search criteria includes misspellings and name derivations).
   - The process used to investigate potential matches.
   - The process used to block and reject transactions.
   - The process used to inform management of blocked or rejected transactions.
   - The adequacy and timeliness of reports to OFAC.
   - The process to manage blocked accounts (such accounts are reported to OFAC and pay a commercially reasonable rate of interest).
   - The record retention requirements (i.e., five year requirement to retain relevant OFAC records; for blocked property, record retention for as long as blocked; once unblocked, records must be maintained for five years).

3. Determine the adequacy of independent testing and follow-up procedures.

4. Review the adequacy of the MSB's OFAC training program based on the MSB's OFAC risk assessment.

5. Determine whether the MSB has adequately addressed weaknesses or deficiencies identified by OFAC or regulators.

TRANSACTION TESTING

1. On the basis of an MSB's risk assessment, prior examination reports, and a review of the independent review, select the following samples to test the OFAC program for adequacy, as follows:

- Sample transactions and evaluate the filtering process used to search the OFAC database (e.g., the timing of the search), and documentation maintained evidencing the searches.
- If the MSB uses an automated system to conduct searches, assess the timing of when updates are made to the system, and when the most recent OFAC changes were made to the system. Also, evaluate whether all of the databases are run against the automated system, and the frequency upon which searches are made. If there is any doubt regarding the effectiveness of the OFAC filter, then run tests of the system by entering test account names that are the same as or similar to those recently added to the OFAC list to determine whether the system identifies a potential hit.
- If the MSB does not use an automated system, evaluate the process used to check the customers against the OFAC list.
- Review a sample of potential OFAC matches and evaluate the MSB's resolution and blocking/rejecting processes.
- Review a sample of reports to OFAC and evaluate their completeness and timeliness

2. Identify any potential matches that were not reported to OFAC, discuss with management, advise management to immediately notify OFAC of unreported transactions, and immediately notify supervisory personnel at your regulatory agency.

3. Determine the origin of deficiencies (e.g., training, independent review, risk assessment, internal controls, management oversight), and conclude on the adequacy of the MSB's OFAC program.

4. Discuss OFAC related examination findings with management.

5. Include OFAC conclusions within the report of examination, as appropriate

RED FLAGS AND MONEY LAUNDERING SCHEMES

Money laundering schemes can vary widely. Federal action to curtail money laundering activities once focused heavily on identification and documentation of large currency transactions and on the use of money transfers, both through bank and non-bank money transfer systems, and other means of moving funds. Today, as money launderers become more sophisticated, all types of financial transactions are facing greater scrutiny.

When a single factor signals that a transaction is unusual and possibly "suspicious," it is called a "red flag." The following are examples of potentially suspicious activities, or "red flags" for both money laundering and terrorist financing. Although these lists are not all-inclusive, they may help MSBs and examiners recognize possible money laundering and terrorist financing schemes. Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing, or a particular crime. Situations like those described in this section often will be found, upon further examination, to be completely legitimate. By the same token, other situations not mentioned here might be suspicious if they are inconsistent with the normal activity of a particular customer or employee. As an MSB or MSB employee, you must make a reasonable judgement.

The following examples are red flags that, when encountered, may warrant additional scrutiny. These lists are not comprehensive, but they may help MSBs recognize ways launderers and other criminals may try to use them to launder money. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Potentially Suspicious Activity That May Indicate Money Laundering

Customers Who Provide Insufficient or Suspicious Information

- A customer uses unusual, false or suspicious identification documents that cannot be readily verified.
- Two/more customers use similar IDs.
- Customer alters transaction upon learning that he/she must show ID.
- Customer alters spelling or order of his/her full name.
- A customer makes frequent or large transactions and has no record of past or present employment experience.

Efforts to Avoid Reporting or Recordkeeping Requirement

- Currency exchanges just under $1,000.
- Cash sales of money orders or traveler's checks of just under $3,000.
- Customer uses two or more locations or cashiers in the same day in order to break one transaction into smaller transactions and evade the BSA reporting or recordkeeping requirement.
- A customer or group tries to persuade an MSB employee to not file required reports or to not maintain required records.
- A customer is reluctant to provide information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.

Funds Transfers

- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds activity is unexplained, repetitive, or shows unusual patterns.
- Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
- Funds transfers are sent or received from the same person to or from different accounts.

Employees

- An employee has lavish lifestyle that cannot be supported by his or her salary.
- An employee fails to conform with recognized policies, procedures, and processes.
- An employee is reluctant to take a vacation.

Activity Not Consistent With the Customer's Business or Occupation

Look for examples of inconsistent customer activity, such as:

- An individual customer conducts MSB transactions in large amounts inconsistent with the income generated by the individual's stated occupation.
- A business customer engages in transactions that frequently use large bills when the nature of the customer's business activity does not justify such use.
- An individual or business customer cashes large numbers of third party checks.
- A customer makes cash purchases of money orders, traveler's checks, or other instruments inconsistent with the customer's business or occupation.
- A business customer uses a means of payment inconsistent with general business practices (e.g., pays for MSB services with traveler's checks, money orders, or third party checks).
- A business customer sends or receives money transfers to/from persons in other countries without an apparent business reason or gives a reason inconsistent with the customer's business.
- A business customer sends or receives money transfers to or from persons in other countries when the nature of the business would not normally involve international transfers.

Unusual Characteristics or Activities

Notice any unusual characteristics, such as:

- An individual customer purchases products/services on a regular basis but seems neither to reside nor work in the MSB's service area.
- A customer pays for MSB products/services using musty bills that have an unusual or chemical-like odor.
- A customer pays for MSB products/services using money orders or traveler's checks without relevant entries on the face of the instrument. (e.g., for money orders — no payee, and for traveler's checks — no signature or countersignature).
- A customer pays for MSB products/services using money orders or traveler's checks with unusual symbols, stamps or written annotations (such as initials) that appear either on the face or on the back of the instruments.
- A customer purchases money transfers, money orders, traveler's checks, etc., with large amounts of cash when the MSB does not require payment in cash.
- An individual or business customer asks to purchase traveler's checks or money orders in large bulk orders.
- A customer purchases a number of money transfers, money orders, or traveler's checks for large amounts or just under a specified threshold without apparent reason.
- A customer starts frequently exchanging small bills for large bills, or vice versa, when the customer does not normally use cash as a means of payment.

Changes in Transactions or Patterns of Transactions

Be alert for changes in activity, such as:

- Major changes in customer behavior, for example: (1) An individual money order customer begins to make weekly purchases of money orders in the same amounts (when previously he or she only purchased money orders on pay day for rent, utilities, etc.). (2) An individual customer begins to bring in large amounts of cash (when previously he or she cashed his or her paycheck to purchase instruments or transfers).
- Sudden and inconsistent changes in money transfer send or receive transactions.
- Rapid increase in size and frequency of cash used by a particular customer.

Summary of Certain Bank Secrecy Act (BSA) Regulations

1. **Registration** — each business that meets the definition of an MSB must register with FinCEN, except for the following:
   - A business that is an MSB solely because it serves as an agent of another MSB;
   - A business that is an MSB solely as an issuer, seller, or redeemer of stored value;
   - The U.S. Postal Service and agencies of the U.S., of any State, or of any political subdivision of any State.
   - A branch office of an MSB is not required to file its own registration form.

   MSBs are required to renew their registration every two years by December 31 at the end of the two-calendar year period following their initial registration. In addition, MSBs that are required to register are also required to prepare and maintain a list of agents, if any, each January 1 for the preceding 12-month period.

2. **Agent List** —
   - MSBs that are required to register must prepare and maintain a list of their agents, if any, each January 1 for the preceding 12-month period.
   - Upon request, MSBs must make their list of agents available to FinCEN and any other appropriate law enforcement or supervisory agencies (including the IRS in its capacity as BSA examination authority).

3. **Suspicious Activity Report (SAR)** — MSBs required to file SARs are:
   - MSBs serving as money transmitters;
   - Currency dealers or exchangers;
   - Issuers, sellers, or redeemers of money orders;
   - Issuers, sellers, or redeemers of traveler's checks; and
   - U.S. Postal Service.

   MSBs must maintain a copy of all SARs filed as well as the original or business record equivalent of any supporting documentation for a period of **five years** from the date of the report. Supporting documentation must be identified as such, and, although it is not to be filed with the report, supporting documentation is deemed to have been filed with the report. Upon request, MSBs must make all supporting documentation available to FinCEN and any other appropriate law enforcement or supervisory agencies (including the IRS in its capacity as BSA examination authority).

   A SAR must be filed by an MSB when a transaction is both:
   - Suspicious, and
   - $2,000 or more ($5,000 or more for issuers reviewing clearance records).

   A SAR must be filed **within 30 days of detection** of the suspicious transaction by the MSB. MSBs that are not currently covered by the SAR rule — check cashers, and issuers, sellers, or redeemers of stored value — may voluntarily file SARs. Any MSB may also voluntarily file SARs for suspicious activity below the reporting threshold.

   <u>It is illegal to tell any person involved in a transaction that a SAR has been filed.</u> Maintaining the confidentiality of SARs will prevent suspected individuals involved in criminal activity from structuring their activity in such a way as to evade detection by law

enforcement. It also will help protect the MSB filing the report. Some suspicious transactions require immediate action. If the MSB has reason to suspect that a customer's transactions may be linked to terrorist activity against the United States, the MSB should immediately call the Financial Institutions Hotline, toll-free at: 1-866-556-3974. Similarly, if any other suspected violations — such as ongoing money-laundering schemes — require immediate attention, the MSB should notify the appropriate law enforcement agency. A BSA provision (called a "safe harbor") provides broad protection from civil liability to MSBs and their employees that file SARs or otherwise report suspicious activity.

All MSBs should have a system or procedure to ensure that SARs are filed when appropriate. When an MSB employee suspects a person is laundering money, conducting transactions to evade BSA requirements, or conducting a transaction that has no apparent lawful purpose and for which no reasonable explanation can be determined, or involves use of the money services business to facilitate criminal activity, the employee should report that activity to his/her manager or to the MSB compliance officer.

4. **Currency Transaction Report (CTR)** — MSBs must file CTRs on transactions in currency involving **more than $10,000**, in either cash-in or cash-out, conducted by, through, or to the MSB on any one day by or on behalf of the same person.

Aggregation - Multiple transactions conducted by or on behalf of the same person on the same day are considered to be one transaction for CTR purposes. In other words, the MSB must file a CTR if it knows the customer's aggregate cash-in or cash-out transactions total more than $10,000 in one day.

Cash-in and Cash-out - Cash-in transactions must be added together with cash-out transactions to determine whether the CTR threshold (greater than $10,000) has been met in anyone business day.

The CTR requirement requires an MSB to:
- Verify and record customer ID,
- Obtain transaction information,
- Complete and file the CTR,
- Retain a copy of the CTR for five years from the date of filing the report.

5. **Monetary Instrument "Log"**— MSBs must maintain certain information on the sale of monetary instruments — such as money orders or traveler's checks — from **$3,000 to $10,000**, inclusive.

The Monetary Instrument "Log" requirement requires an MSB to:
- Verify and record customer ID,
- Record transaction information (for each money order, traveler's check, or other instrument purchased: amount, serial number, and date sold),
- Retain the record for five years from the date of the transaction.

6. **Funds Transfer Rules** — MSBs must maintain certain information for funds transfers, such as sending or receiving a payment order for a money transfer, of **$3,000 or more**, regardless of the method of payment.

For Receivers of Money Transfers - An MSB that accepts an instruction to pay a money transfer of $3,000 or more must verify the identity of the receiving customer and create and maintain a record of the money transfer, regardless of the method of payment.

The requirement to record funds transfers requires a money transmitter to:

- Verify customer ID,
- Record customer information,
- Record transaction information,
- Send information to receiving MSB,
- Retain the record for five years from the date of the transaction.

7. **Currency Exchange Record**— MSBs must maintain certain records for each currency exchange in excess of $1,000.

8. **Record Retention** — All BSA records must be retained for a period of **five years** and must be filed or stored in such a way as to be accessible within a reasonable period of time.

Civil and Criminal Penalties

Civil and criminal penalties can be imposed for violations of anti-money laundering laws and regulations. Penalties can result in substantial fines and in prison terms. Any MSB that fails to comply with BSA reporting and record keeping requirements faces possible civil penalties of up to $500 for negligent violations and the greater of the following two amounts for willful violations: the amount involved in the transaction (up to $100,000) or $25,000. Under certain circumstances, businesses can also be held criminally liable for the acts of their employees.

The maximum criminal penalty for violating a BSA requirement is a fine of up to $500,000 or a term of imprisonment of up to 10 years, or both. It is therefore important that employees are thoroughly trained on how to comply with BSA regulations and that a system is in place to ensure that employees are following all anti-money laundering laws and regulations. MSBs can do a great deal to help the federal government in its anti-money laundering efforts. At a minimum, MSBs should file all BSA reports accurately and in a timely fashion, create and maintain accurate BSA records for the requisite time period, establish and maintain appropriate compliance programs and follow all Treasury Department guidance related to the BSA.