LAWDESK

BANK SECRECY ACT AND ANTI-MONEY LAUNDERING

TRAINING

BSA/AML Training

Introduction

The *Bank Secrecy Act* ("BSA") and Anti-Money Laundering ("AML") rules are intended to protect the U.S. financial system and the financial institutions that make up that system from the abuses of **financial crime**s, including **money laundering**, **terrorist financing**, and other **illicit financial transactions**. Money laundering and terrorist financing are financial crimes with potentially devastating effects. In both money laundering and terrorist financing, criminals can exploit loopholes and other weaknesses in the legitimate financial system to launder criminal proceeds, finance terrorism, or conduct other illegal activities, and, ultimately, hide the actual purpose of their activity.

This is why it is so important for financial institutions to develop, implement, and maintain effective BSA/AML programs that address the ever-changing strategies of money launderers and terrorists who attempt to gain access to the U.S. financial system. A sound BSA/AML compliance program is critical in deterring and preventing these types of activities at, or through, financial institutions.

Money Laundering

Money laundering is the criminal practice of filtering money obtained from illegal activities through a series of transactions, so that the funds are "cleaned" to appear as though they came from legitimate activities. Money laundering involves three independent steps that can occur simultaneously:

1. **Placement** involves getting the "dirty" money into the financial system without attracting law enforcement. Examples include dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account; depositing a refund check from a canceled vacation package or insurance policy; or purchasing a series of monetary instruments (e.g., cashier's checks or money orders) that are then collected and deposited into accounts at another location or financial institution.

2. **Layering** involves moving the money, often in a complex series of transactions, to complicate the paper trail. Examples include exchanging monetary instruments for larger or smaller amounts; or wiring or transferring funds to and through numerous accounts in one or more financial institutions.

3. **Integration** involves using the money to create the appearance that the money is "clean". Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets.

Terrorist Financing

Terrorist financing provides funds for terrorist activity. It may involve funds raised from legitimate sources, such as charitable donations, foreign government sponsors, business ownership, and personal employment, as well as from criminal sources, such as extortion, kidnapping, narcotics trafficking, smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds, and improper use of charitable or relief funds.

Terrorists use the same or similar methods to those of money launderers to evade authorities' attention and to protect the identity of their sponsors and of the ultimate beneficiaries of the funds. For example, terrorist financiers use currency smuggling; structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers.

However, financial transactions associated with terrorist financing tend to be in smaller amounts than is the case with money laundering, and when terrorists raise funds from legitimate sources, the detection and tracking of these funds becomes more difficult.

Penalties

Penalties for money laundering and terrorist financing can be severe. Anyone charged with the crime of money laundering can face **up to 20 years** in prison and fines **up to $500,000**. Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property, and even entire bank accounts may be subject to forfeiture.

Financial institutions and individuals may face criminal and civil liability for violating **AML and terrorist financing laws**. Those penalties may include **multimillion dollar fines**, **imprisonment**, and **forfeiture** actions. Additionally, **financial institutions** risk losing their charters and financial institution **employees** risk being removed and barred from banking.

BSA/AML Compliance Program

A financial institution's BSA/AML compliance program must be in writing and approved by its board of directors. It must be commensurate with its risk profile.

At minimum, BSA/AML compliance programs must contain:

1. **Internal Controls -** Policies, procedures, and processes designed to limit and control risks and to achieve compliance with BSA.

2. **BSA Compliance Officer -** A specifically designated individual(s) responsible for managing BSA compliance.

3. **Independent Testing -** Independent testing to verify program effectiveness.

4. **Training -** Training of appropriate personnel on regulatory requirements and the institution's internal BSA/AML policies, procedures, and processes.

Customer Identification Program

An important element of BSA/AML compliance is ensuring that you have obtained enough information from a customer to properly identify that person. The rules require you to **obtain** certain minimum pieces of identification from individuals and businesses. You must also provide **notice** to customers that identity verification will occur.

To open an **account for an individual**, you must collect:

1. Name
2. Date of birth
3. Street address (cannot be a Post Office Box)
4. Identification number:

    - U.S. citizens must provide a Taxpayer Identification Number (TIN). Example: Social Security Number (SSN).

    - Non-U.S. citizens must provide one or more of the following:

        a. TIN
        b. Passport number and country of issuance
        c. Alien identification card number
        d. Number and country of issuance of any other government-issued photo ID

To open an **account for a business** or other entity, you must collect:

1. Name
2. Address of principal place of business (local office or other physical location)
3. Identification number:

- U.S. organizations must provide a Taxpayer Identification Number (TIN). Example: Employer Identification Number (EIN).

- Foreign organizations must provide either a TIN or a government-issued document certifying the entity's existence.

Once you collect the identifying information, **you must verify it**. You can do this by:

1. **Reviewing documents** - For an individual, use a valid (not expired), government-issued photo ID (Examples: driver's license, passport). For a business or other entity, check documents, such as articles of incorporation, business license, partnership agreement and association bylaws.

2. **Checking Fraud** and bad check databases to make sure the party is not listed.

3. **Comparing Information** to a trusted third-party source (Example: a credit report).

4. **Looking for consistency of information** throughout provided documents, such as the name, address, date of birth, SSN, etc. (Examples: does the date of birth match the credit report? does the SSN sequence match the state issuing the SSN?)

Customer Due Diligence

Customer due diligence ("CDD") is about getting to know your customer. It enables you to predict the types of transactions in which a customer is likely to engage and assists in determining when transactions are potentially suspicious.

CDD begins with verifying the customer's identity and assessing the risks associated with that customer by obtaining information about the nature and background of the account. Customers posing a higher-risk for money laundering or terrorist financing must be subject to enhanced CDD.

Institutions are expected to monitor their customers through regular suspicious activity monitoring and customer due diligence processes. If there is indication of a potential change in the customer's risk profile (e.g., expected account activity, change in employment or business operations), the customer risk rating should be reassessed.

In the CDD process, you should collect information about the background and nature of the account. This process should include evaluating:

1. The purpose of the account [or the second part?]
2. Actual or anticipated activity in the account
3. Nature of the customer's business/occupation
4. Customer's location
5. Types of products and services used by the customer

Much of this information can be confirmed through:

- Information-reporting agencies
- Banking references
- Correspondence and telephone conversations with the customer
- Visits to the customer's place of business
- Third-party references
- Public information (e.g., on the Internet or commercial databases)

Certain **products and services**, **customers and entities**, and **geographic locations** may pose higher risks. However, the risks are not always the same, various factors must be considered. Therefore, each financial institution has the discretion to decide who and what it considers high-risk.

Enhanced Due Diligence

When a customer is identified as higher-risk, the rules require **enhanced due diligence** ("EDD"). EDD involves collecting and verifying information beyond the minimum.

At account opening and throughout the relationship, you should obtain customer information such as:

Due diligence is an ongoing process
you should take measures to ensure account profiles are current and monitoring is risk-based.

Your institution should consider whether risk profiles should be adjusted or suspicious activity reported through a *Suspicious Activity Report* ("SAR") when the activity is inconsistent with the profile attributes, such as:

- Purpose of the account
- Source of funds and wealth
- Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors
- Occupation or type of business
- Financial statements
- Banking references
- Domicile (where the business is organized)
- Proximity of customer's residence, place of employment, or place of business to the institution
- Description of the customer's primary trade area and whether international transactions are expected to be routine
- Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers
- Explanations for changes in account activity.

Suspicious Activity Reporting

Suspicious activity reporting is the foundation 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. We use a number of methods to identify potentially suspicious activity.

One of **the most important methods is YOU**.

Therefore, it is vital for you to always be on the lookout for potentially suspicious activities or red flags and follow your institution's procedures when encountering a red flag. Remember, a **red flag** may not by itself evidence criminal activity. Closer scrutiny of the red flag will help to determine whether the activity is suspicious.

To identify whether activity is suspicious, ask yourself the below question. If the answer to any of these questions is yes, the activity is a **"red flag"** and requires further investigation.

Based on your knowledge of the accountholder or account history, is the transaction:

- Larger than a typical transaction?
- More complex than normal?
- Inconsistent with the account history?
- Unusual in any other way?

Red Flags

During the course of day-to-day operations, you may observe unusual or potentially suspicious activity. Here are some categories of **"red flags"** of suspicious activity.

- **Customers who provide insufficient or suspicious information** - Red flags involving customer information and documentation that should raise your suspicion include:

    - Unusual or questionable identification that cannot be easily verified
    - Different social security numbers with name variations.
    - Home or business telephone numbers that have been disconnected.
    - Using a nonlocal residential or business address.
    - A new business is reluctant to provide information about the nature of the business, names of its officers and directors, prior banking relationships, or its business location.
    - Past or present employment experience is inconsistent with the number and amount of transactions.

- **Efforts to avoid reporting or record keeping requirements** - Red flags involving customers or groups avoiding the CTR or SAR reporting and record keeping requirements include:

    - Requesting to be exempt from filing. Persuading a bank employee to not file a report or asking questions about how to avoid having a report filed.
    - Refusing to provide the required documentation to file the report. Changing the amount of a transaction after learning a report is to be filed.
    - Using the automatic teller machine at multiple locations to make several bank deposits below the threshold amount.
    - Depositing funds into several accounts in increments of less than $3,000.
    - Requesting several small denomination cashier's checks when redeeming a certificate of deposit.
    - Reluctant to provide identification when purchasing monetary instruments in recordable amounts.

- **Funds transfers** - Red flags involving wire or funds transfers include:

    - Transactions that are inconsistent with the business or account. Unusual activity patterns that are unexplained or repetitive. (e.g., high-dollar incoming wires from foreign countries to a cash-intensive convenience store business)
    - Transfers where the source of funds is not apparent (e.g., high-dollar wires going out of accounts with low deposits and low average balances)
    - Numerous small incoming transfers or deposits made with money orders, travelers or cashier's checks.
    - Transfer activity between and among accounts with the beneficial owner, for no apparent reason.
    - A large outgoing wire just after an account is opened or cash deposits followed by an immediate request for outgoing wires.

- **Lending activity** - Red flags involving suspicious lending activity include:

    - Reluctance to provide the purpose of the loan or the stated purpose is ambiguous.
    - Inconsistent or inappropriate use of loan proceeds (e.g., a borrower states home improvement as the loan purpose but you later learn the proceeds were used to purchase a boat).
    - Loans to non-U.S. borrowers.
    - Involvement of third parties (e.g., payment made by third parties, collateral pledged by third parties, or proceeds used to purchase property to be held in the name of third parties).

- **Changes in bank-to-bank transactions** - Red flags involving transactions between unaffiliated banks include:

    - Rapid increase in the number and dollar amount of currency deposits.
    - Unable to trace the origins of the deposits.
    - Frequent exchange of small denomination bills to large denomination bills is unusual considering the bank's location.

- **Insurance** - Insurance red flags include:

    - Purchasing products with termination features without concern for the product's investment performance.
    - Purchasing insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.
    - Purchasing a product that appears outside the customer's normal range of financial wealth or estate planning needs.
    - Borrowing against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.
    - Purchasing policies that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer (including secondhand endowment and bearer insurance policies).
    - Purchasing several insurance products and using the proceeds from an early policy surrender to purchase other financial assets.
    - Using multiple currency equivalents (e.g., cashier's checks and money orders) from different banks and money services businesses to make insurance policy or annuity payments.

- **Shell company activity** - Red Flags involving shell company activity include:

    - The purpose of the shell company is unclear.
    - Inability to obtain any information necessary to identify the originators or beneficiaries of wire transfers into the shell company account.
    - Payments to or from the shell company do not reference goods or services and have no stated purpose.
    - Goods or services of the shell company do not match the company's profile based on the information previously provided to the financial institution.
    - An usually large number and a variety of beneficiaries receive wire transfers from one company.
    - Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.

- **Employees** - Red flags involving co-workers or employees include:

    - Employee exhibits a lavish lifestyle that cannot be supported by their salary.
    - Employee fails to conform to recognized policies, procedures, and processes, particularly in private banking.
    - Employee is reluctant to take a vacation.

- **Deposits** - Red flags involving suspicious deposit activity include:

    - Transactions inconsistent with the accountholder's business or income level (e.g., a municipal worker opens a checking account with a large amount of traveler's checks).
    - Opening accounts where the source of funds is not readily apparent (e.g., a student opens an account with a large amount of cash).
    - Opening multiple accounts for no apparent legitimate reason.
    - Activity across multiple accounts just under reporting thresholds or involving monetary instruments (e.g., a customer maintains several accounts and scatters activity among them with no apparent reason for the practice).
    - Unusually large deposits of food stamps into business or retail accounts. Inconsistent deposit and withdrawal activity.

- **Safe Deposit Boxes** - When interacting with accountholders who want access to safe deposit boxes, some red flags you may notice are:

    - Frequent visits to the safe deposit box before or after large cash deposits or withdrawals.
    - People from outside the local area opening safe deposit boxes.
    - Renting multiple safe deposit boxes.

- **Monetary instruments** - Unusual monetary instrument purchase patterns can also be red flags for money laundering. Be alert for:

    - Individuals or groups purchasing monetary instruments with large amounts of cash and structuring their purchases to fall below the reporting or logging threshold. (e.g., purchasing monetary instruments at multiple locations to avoid logging or reporting).
    - Depositing or purchasing multiple monetary instruments simultaneously.
    - Providing incomplete or false information when purchasing instruments.

- **Other unusual or suspicious activity** - Additional suspicious activities to be alert for:

    - Customer purchases a number of open-end prepaid cards for large amounts.
    - Customer receives frequent deposits from online payments systems and has no apparent online business.
    - International transfers from or to higher-risk locations.

Suspicious Activity Reporting

Financial institutions must file a ***Suspicious Activity Report*** ("SAR") if a transaction involves or aggregates **$5,000 or more** and it:

- Involves funds derived from an illegal activity.
- Is designed to evade a reporting requirement.
- Appears to have no business or lawful purpose.

All SARs must be filed electronically.

A SAR must be filed within **30 calendar days after the initial detection of facts that support the SAR filing**. In other words, a SAR must be filed within 30 calendar days of identifying suspicious activity that meet the thresholds of filing a SAR.

If you cannot initially identify a suspect, you may delay an **additional 30** calendar days to attempt to identify the suspect.

You should **never reveal** to anyone (other than your supervisor if necessary) that a SAR may be or has been filed! Filing is strictly confidential. Disclosing that a SAR has been or may be filed violates the rules.

In situations requiring immediate attention, such as an ongoing criminal violation, a financial institution must immediately notify the appropriate **law enforcement** agency by telephone. Shortly thereafter, institutions must also notify its **primary regulator** by phone or in writing.

It is important to note that informing law enforcement does not remove the obligation to file a SAR. A SAR must be filed even if law enforcement is informed and an investigation is started.

The narrative section of the SAR - is a critical compliance tool. It must be properly and thoroughly completed to provide law enforcement with a sufficient description of the suspicious transaction.

You may attach to the SAR a Microsoft Excel compatible comma separated values (CSV) file with no more than one megabyte of data to document transaction records that are too numerous to record in the narrative section. No other supporting documentation should be attached to the SAR. However, all necessary supporting documents should be identified and retained with a copy of the SAR.

Because the SAR narrative is so important, your role is to provide as much detail as possible about the suspicious activity to your supervisor or manager so that the narrative can be completed properly.

Currency Transaction Reports

A *Currency Transaction Report* ("CTR") must be filed for **cash transactions** of **more than $10,000** on any **one business day** when there is:

- Cash in,
- Cash out, or
- Currency exchanged.

Cash in is an account deposit or a loan payment made with currency.

Cash out could be an account withdrawal or a loan disbursement or advance taken in currency. All CTRs must be filed electronically.

Currency is - **coin** and **paper money** of the United States or any other country.

Currency is not - any other type of funds. Checks, drafts, traveler's checks and money orders are not cash. Electronic transactions, such as ACH debits or wire transfers, are not currency transactions.

If **cash transactions** conducted "by or on behalf of" the same individuals or entities in one business day exceed $10,000, a CTR is required.

Cash in and cash out are not netted together for reporting purposes. **If the total amount of cash in, cash out or currency exchanged exceeds the $10,000 reporting threshold, a CTR is required**. **Structuring** (deliberately breaking up cash transactions to avoid a CTR) is illegal.

A CTR is not required in processing cash from:

- Federal Reserve Banks
- Banks or Credit Unions
- Government Entities

The financial institution must file the CTR within **15 calendar days** of the reportable transaction.

You should also be aware that **some account holders may be exempted from CTR filings**. Those entities eligible for exemption are entities listed on a major national stock exchange (NYSE, AMEX, NASDAQ) and their subsidiaries, entities who have an established account history, and whose business type is cash-intensive (such as retail stores), and payroll customers.

These account holders must meet certain criteria, in addition to filing and review requirements, in order to be exempted from filing. Be sure to check your institution's procedures to learn about exempt entities.

Even if an entity is exempt from CTR reporting, you must still file a Suspicious Activity Report (SAR) if suspicious activity is detected!

Monetary Instruments Recordkeeping

Financial institutions sell a variety of monetary instruments in exchange for currency. **Monetary instruments include:**

- cashier's checks
- traveler's checks
- drafts
- money orders

The rules require financial institutions to maintain records of monetary instruments purchased with **cash** between **$3,000 and $10,000**.

You must add same-day purchases together for recordkeeping purposes. The same rule applies as for CTRs: if the purchase is "by or on behalf" of the same parties in the same business day and the total is between $3,000 and $10,000, recordkeeping requirements apply.

Funds withdrawn from an account or the proceeds of a cashed check used to make such purchases are not considered cash purchases. However, when a customer purchases a monetary instrument using cash that the customer first deposits into an account, it is subject to the recordkeeping requirements.

The information you must collect depends on whether or not the purchaser has a deposit account with your institution.

Accountholders

- Name of purchaser
- Date of purchase
- Type of instruments purchased
- Serial number of each of the instrument purchased
- Amount of each of the instruments purchased

Non-Accountholders

- Name and address of purchaser
- SSN or alien ID number of purchaser
- Date of birth of purchaser
- Date of purchase
- Type of instruments purchased
- Serial number of each of the instruments purchased
- Amount of each of the instruments purchased
- Specific ID information for verifying the purchaser's identity (e.g., state of issuance and number of driver's license)

Funds Transfer Recordkeeping

The BSA/AML rules require financial institutions involved in funds transfers to collect and retain certain information. The information required to be collected and retained depends on whether your institution is the:

1. **Originating Institution** - A financial institution that accepts and processes a **payment order (i.e., outgoing wire)**. The Originator is a person or entity who requests a payment order. A payment order or transmittal order is an order to transfer funds from one party to another.

2. **Intermediary Institution** - A financial institution that passes a payment order from an originating institution to a beneficiary's institution. Some funds transfers bypass the intermediary institution and go directly to the beneficiary's institution.

3. **Beneficiary's Institution** - A financial institution that receives a payment order and delivers the transfer proceeds to a beneficiary. The *Beneficiary* is a person or entity who receives the proceeds of a funds transfer.

(1) Originating Institution

When an **established customer** requests a **payment order (i.e., outgoing wire)** of **$3,000 or more**, you must collect and retain certain minimum information (*see* bold categories). The minimum information required includes: name and address of the originator; amount of the payment order; date of the payment order; payment instructions; identity of the beneficiary's institution; and any other information specifically identifying the beneficiary that the originating institution may receive with the payment order.

For established customers, information must be retrievable by originator name and account number.

WIRE TRANSFER REQUEST		
	Transfer Date (Payment Order)	08/05/20XX
	Originator Name & Address	Josh Mitchell Address
	Originator Account Number	01-10543546
	Originator Address	5421 West 14th Avenue Anytown, USA 00000
	Originator Phone Number	502-555-5431
	Originator Tax ID Number	546-54-6546
	Originator ID #1	USA DL 2165479002
	Originator ID #2	US Passport 546-54-6546
	Payment Instructions	PUPID
	Transfer Amount (Amount of Payment Order)	$15,000
	Transfer Fee Collected (1%)	$150
	Transfer Funds	Cash
	Beneficiary	Kari Oksanen (Any information obtained)
	Beneficiary Address	23 Suomentie #456 Helsinki, Finland 00000
	Transfer Beneficiary Financial Institution	Bank of Finland
	Transfer Recipient Acct #	6546329901

If the originator is **not an established customer**, you must collect and retain the information listed on the above. In addition, you must collect and retain other information, depending on whether the payment order is made in person. For non-customers, information must be retrievable by originator name.

In Person - If the payment order is made in person, you must verify the identity of the person placing the payment order before you accept the order, then obtain and retain:

- Name and address of the person placing the order;
- Type of identification reviewed;
- Number of the identification document; and
- The person's taxpayer identification number (e.g., Social Security Number (SSN) or Employer Identification Number(EIN))

Not In Person - If a payment order is not made in person, you must obtain and retain:

- Name and address of the person placing the order; and
- The person's taxpayer identification number (e.g., SSN or EIN)

Travel Rule

For funds transmittals of **$3,000 or more**, you must include the following information in the transmittal order at the time that a transmittal order is sent to a receiving financial institution.

- Name of the transmitter
- The account number from which the payment is ordered, if applicable
- Address of transmitter
- Amount of transmittal order
- Date of the transmittal order
- Identity of the recipient's financial institution
- As many of the following items as are received with the transmittal order:
    - Name and address of the recipient
    - Account number of the recipient
    - Any other specific identifier of the recipient
- Either the name and address or the numerical identifier of the transmitter's financial institution

(2) Intermediary Institution

If a financial institution is acting as an intermediary institution in a wire transfer, it means that it must pass along all information received from the originating institution to the beneficiary's institution. However, an intermediary institution has no duty to obtain information related to the transaction that was not provided by the originating institution.

An intermediary institution must retain records of each **payment order (i.e., outgoing wire)** of **$3,000 or more** that it accepts.

(3) Beneficiary Institution

For each **payment order (i.e., outgoing wire)** of **$3,000 or more** that an institution accepts as a beneficiary's institution, it must retain a record of that order.

If the beneficiary is **not an established customer**, it must retain certain information for each payment order of $3,000 or more, depending on whether or not the proceeds are delivered in person.

Information retained must be retrievable by reference to the name of the beneficiary. When the beneficiary is an established customer and has an account used for funds transfers, information retained must also be retrievable by account number.

In Person - If proceeds are delivered in person to the beneficiary or its representative or agent, you must verify the identity of the person receiving the proceeds and retain:

- Name and address;
- Type of identification reviewed;
- Number of the identification document;
- The person's taxpayer identification number (e.g., SSN or EIN) or a notation in the record of the lack thereof; and
- If you have knowledge that the person receiving the proceeds is not the beneficiary, you must obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's identification.

Not In Person - If proceeds are not delivered in person, you must:

- Retain a copy of the check or other instrument used to make the payment; or
- Record the information on the instrument; and
- Record the name and address of the person to whom it was sent.

The Office of Foreign Assets Control ("OFAC")

OFAC enforces economic and trade sanctions against **individuals**, **entities** and **foreign governments** with interests that are hostile to the United States. OFAC publishes a list that identifies those parties with whom transactions are prohibited. The Department of the Treasury updates the list as necessary.

The OFAC list is **not just a list of terrorists**. It also includes those suspected of money laundering, narcotics trafficking and other crimes, as well as governments or organizations with interests that are hostile to the United States.

OFAC rules require financial institutions and their employees to:

- Identify any property or transaction subject to economic sanctions
- Block or reject the transaction
- Freeze an account
- Advise OFAC of the blocked asset or rejected transaction
- Release the blocked transaction or property only on OFAC's authorization

Most financial institutions have automated systems that compare requested transactions against the OFAC database. Institutions must also have procedures in place concerning what you should do if a potential match, or "hit", is detected.

Generally, when a "**hit**" is identified, you must perform additional steps, which **may** include **blocking or rejecting the transaction**. If you get a "hit" against the list (an exact or very close match) you must take additional steps to determine whether the individual or entity to whom you are providing services is the same as the one named on the list.

If many similarities are present, OFAC should be contacted for further verification (Example: The name is an exact match, and the general location listed is the same). Involve your manager or supervisor in this type of situation.