ANTI-MONEY LAUNDERING COURSE
# Table of Contents

**INTRODUCTION** ........................................................................................................................................................................ 1  
Money Laundering Defined .............................................................................................................................................................. 1  
Scope of Money Laundering ............................................................................................................................................................ 1  
Government Efforts to Combat Money Laundering in the United States. ......................................................................................... 1  
Bank Secrecy Act (BSA) ....................................................................................................................................................................... 2  
The USA Patriot Act ............................................................................................................................................................................ 2  
Anti-money Laundering Laws ............................................................................................................................................................ 2  
Course Description............................................................................................................................................................................. 2  
Course Learning Objectives............................................................................................................................................................... 2  

**SECTION 1** ........................................................................................................................................................................................................... 4  
The Basics of Money Laundering ........................................................................................................................................................ 4  
Knowledge Base - Terms and Acronyms ............................................................................................................................................ 4  
Terrorist Financing .............................................................................................................................................................................. 4  
Office of Foreign Asset Control (OFAC) ........................................................................................................................................ 4  
Specially Designated Nationals (SDN) .............................................................................................................................................. 4  
Financial Crimes Enforcement Network (FinCEN) ............................................................................................................................ 4  
Financial Action Task Force (FATF) .................................................................................................................................................. 5  
Suspicious Activity Report (SAR) ...................................................................................................................................................... 5  
Covered Insurance Companies and Products ................................................................................................................................... 5  
Know Your Customer (KYC) ............................................................................................................................................................. 6  
Cash ........................................................................................................................................................................................................... 6  
Cash Equivalents .................................................................................................................................................................................. 6  
The Stages of Money Laundering ....................................................................................................................................................... 7  
Placement .......................................................................................................................................................................................... 7  
Layering ............................................................................................................................................................................................ 7  
Integration .......................................................................................................................................................................................... 7  
How Terrorist Financing Differs From Traditional Money Laundering ............................................................................................ 8  

Section 1 - Review Questions ................................................................................................................................................................. 9  

**SECTION 2** .................................................................................................................................................................................................................. 11  
AML Rules & Regulations .................................................................................................................................................................... 11  
USA Patriot Act Title III ....................................................................................................................................................................... 11  
Section 326 of USA Patriot Act Title III ........................................................................................................................................... 11  
Section 352 of USA Patriot Act Title III........................................................................................................................................... 11  
AML Programs Must be .......................................................................................................................................................................... 11  
Examples of High-risk Customers .................................................................................................................................................... 12  
Examples of High-risk Businesses .................................................................................................................................................... 12  
Reporting of Suspicious Activity ...................................................................................................................................................... 13  

Section 2 - Review Questions ................................................................................................................................................................. 14
SECTION 3

Agent & Broker Responsibilities Under AML Regulations

Gain Familiarity With Company AML Programs
Payment Methods
Payment Methods Example 1
Payment Methods Example 2
Payment Methods Example 3
Red Flags Can Alert an Agent to Suspicious Activity
Partial List of Red Flags
Know Your Customer (KYC)
Information Required for Customer Identification
Acceptable Documents for Identification of an Individual
Acceptable Documents for Identification of a Business Entity
Non-Documentary Identity Verification

Section 3 - Review Questions

SECTION 4

Reporting Suspicious Activity and Consequences for Non-Compliance

Identification and Reporting of Suspicious Activity
Insurance Agents Contractually Obligated to Report Suspicious Activity
Required Reporting of Suspicious Transactions
Voluntary Reporting of Suspicious Transactions
Required Reporting of Cash Transactions over $10,000
Protection From Liability for Reporting Activity as Suspicious
Record Keeping Requirements
Consequences of Non-Compliance
Civil Penalties
Willful Blindness
Civil Penalties
Loss of Insurance Company Appointment
Damage to Reputation

Section 4 - Review Questions
Introduction

MONEY LAUNDERING DEFINED

The term “money laundering” is generally regarded as the practice of engaging in financial transactions to conceal the identity, source, and/or destination of illegally gained money. Essentially, the proceeds of crime are converted into assets which appear to have a legitimate origin.

Federal law makes it illegal for financial institutions, including insurance companies, to engage in money laundering.

SCOPE OF MONEY LAUNDERING

The crime of money laundering is perpetuated by many types of criminals such as terrorists, drug traffickers, embezzlers, corrupt politicians, tax evaders, con artists, weapons traffickers and individuals involved in the illicit trafficking and exploitation of human beings.

By its very nature, money laundering occurs outside the normal range of economic and financial activities making it difficult to generate accurate estimates of the volume of money laundering that occurs.

The effort against money laundering has been a cornerstone of the global fight against crime since the late 1980s. The fundamental objective of this effort is to ensure that criminal misuse of the financial system is detected and defeated. Confronting terrorist financing has taken on new urgency since the terrorist attacks in 2001.

To give the reader a sense of the scale of enforcement efforts to prosecute money laundering, in 2010 the Internal Revenue Service initiated 1597 money laundering investigations which resulted in 751 individuals being sentenced to an average of 69 months in prison.

Money laundering is an evolving activity, and criminals are constantly developing new strategies to avoid detection while regulators are continually developing new techniques to detect these strategies.

GOVERNMENT EFFORTS TO COMBAT MONEY LAUNDERING IN THE UNITED STATES.
**Bank Secrecy Act (BSA)**

The Bank Secrecy Act, enacted in 1970, authorizes the Secretary of the Treasury to require certain records or reports where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.

The Bank Secrecy Act requires many financial institutions (including covered insurance companies) to have a written program approved by the board of directors. This program must be reasonably designed to effect and monitor compliance with the BSA. Minimum requirements for this program include:

- A system of internal controls to ensure continuous compliance
- Testing of compliance by an independent method
- Designating an individual as responsible for monitoring compliance
- Ongoing training for personnel

**The USA Patriot Act**

In response to the September 11, 2001 terrorists attacks, Congress passed the USA Patriot Act. This act strengthens U.S. anti-money laundering laws and enhances criminal and civil penalties for violations. It also granted new law enforcement powers and surveillance opportunities. The intent of the USA Patriot Act is to identify and track terrorists and persons or entities using U.S. financial institutions to further their causes and also to prevent money laundering by terrorists or other criminal organizations.

**Anti-money Laundering Laws**

For the purposes of this course we will occasionally refer to the Bank Secrecy Act and The USA Patriot Act collectively as Anti-money Laundering Laws or AML laws.

**Course Description**

This course is designed to inform the insurance producer of the responsibilities and duties of life insurance companies and producers in combating money laundering as required by the USA Patriot Act.

This course is broken into four sections, and at the end of each section you will be presented with review questions related to that section. The final exam for this course is comprised of five case scenarios with multiple choice answers designed to test your mastery of the entire course. You must score 80% or better on the final exam in order to pass the course.

**Course Learning Objectives**
Learn important terms and concepts necessary to understand the most common strategies employed by criminals in the perpetuation of the crime of money laundering.

Explore prevention, detection, and enforcement techniques used by insurance companies, producers and regulatory entities against the crime of money laundering.

Develop an understanding of the role and responsibilities of the insurance producer in preventing money laundering.
Section 1

The Basics of Money Laundering

KNOWLEDGE BASE - TERMS AND ACRONYMS

In this section of the course we will build a knowledge base by learning some of the terms commonly encountered when discussing the detection and prevention of money laundering in the insurance industry.

TERRORIST FINANCING

Terrorist financing involves the use of money to fund illegal activities. These funds may have been obtained lawfully or unlawfully. Since these transactions often have a legitimate source and are often small in amount, terrorist financing can be more difficult to detect than other money laundering transactions. An effective anti-money laundering program can help prevent the use of legal or illegal funds for terrorist financing.

OFFICE OF FOREIGN ASSET CONTROL (OFAC)

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or economy of the United States.

SPECIALY DESIGNATED NATIONALS (SDN)

OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called Specially Designated Nationals or SDNs. Their assets are blocked and U.S. persons and financial institutions are generally prohibited from dealing with them.

FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN)

The U.S. Department of the Treasury established the Financial Crimes Enforcement Network in 1990 to provide a government-wide multi-source financial intelligence and analysis network. The organization's operation was broadened in 1994 to include regulatory responsibilities for administering the Bank Secrecy Act.
The Bank Secrecy Act, enacted in 1970, authorizes the Secretary of the Treasury to require certain records or reports where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.

**FINANCIAL ACTION TASK FORCE (FATF)**

The Financial Action Task Force (FATF) is an international anti-money laundering organization whose purpose is the development and promotion of policies to combat money laundering and terrorist financing, both at national and international levels.

The FATF monitors the progress of member countries in implementing necessary measures, reviews money laundering and terrorist financing techniques and countermeasures, and promotes the adoption and implementation of appropriate measures globally.

**SUSPICIOUS ACTIVITY REPORT (SAR)**

Suspicious activity reports are one of the government’s main weapons in the battle against money laundering and other financial crimes because these reports generate leads that law enforcement agencies use to initiate money laundering investigations. Insurance companies file a SAR regarding suspicious or potentially suspicious activity with FinCEN.

**COVERED INSURANCE COMPANIES AND PRODUCTS**

Not all insurance companies or insurance products are covered by the AML Laws. The treasury department determined that the greatest money laundering risk was posed by insurance products with investment features or the ability to store value that can be transferred. The definition of an insurance company covered by the AML laws includes a company in the United States that is engaged in ANY of the following:

- Issuing, underwriting, or reinsuring a life insurance policy.
- Issuing, granting, purchasing, or disposing of an annuity contract.
- Issuing, underwriting, or reinsuring “any insurance product with investment features similar to those of a life insurance policy or an annuity contract, or which can be used to store value and transfer that value to another person.

Life insurance and annuity products considered **Covered Products** by the AML laws:

- A permanent life insurance policy, other than a group life insurance policy.
- An annuity contract, other than a group annuity contract (or charitable gift annuity).
• Any other insurance product with features of cash value or investment.

Life insurance and annuity products NOT considered Covered Products under the AML laws:

• Group life insurance
• Group annuities
• Term life insurance

NOTE: Consult your insurance company for guidance on which of their products are considered Covered Products.

Other insurance products that are exempt from the AML laws include products that the Department of the Treasury has determined pose a low risk for money laundering, such as health, property & casualty, and mortgage insurance.

KNOW YOUR CUSTOMER (KYC)

Knowing your customer involves compliance with the AML laws as they relate to proper identification of the client and gathering relevant information pertinent to doing financial business with them.

CASH

As simple as it seems, it is important to define the term cash. When used in discussions related to anti-money laundering efforts, the term “cash” refers to currency (U.S. or foreign). Many insurance companies, as a matter of policy, will not accept cash for the payment of premiums. Cash is often used in the Placement Stage of money laundering. The stages of money laundering will be discussed later in this course.

CASH EQUIVALENTS

When used in discussions related to anti-money laundering efforts the term “cash equivalents” refers to financial instruments such as money orders, traveler’s checks and cashier’s checks. As part of their AML compliance programs, many insurance companies either will not accept cash equivalents or will require a legitimate, well-documented reason for the use of cash equivalents. When cash equivalents are accepted by an insurance company, they are often subject to limits and are reviewed on a case-by-case basis.

Cash equivalents are often used in the Placement Stage of money laundering. The stages of money laundering will be discussed later in this course.
THE STAGES OF MONEY LAUNDERING

The process of money laundering can be divided into three basic stages:

**PLACEMENT**

The first stage of money laundering involves injecting the illicit funds (usually cash) into the financial system. The launderer inserts the illicit cash into a legitimate financial institution by depositing it into a bank or by purchasing a life insurance policy or annuity with cash. Due to reporting requirements for cash transaction and additional scrutiny by insurance companies, this is a risky process for the launderer. Another common strategy employed by money launderers is to convert illicit cash into financial instruments, such as money orders or traveler’s checks, and combine these instruments with legitimate funds to avoid detection.

In an effort to circumvent the cash transaction reporting requirements some launderers will often structure deposits. Structuring deposits involves breaking a large cash amount into several smaller amounts. In the United States, this smaller amount has to be below $10,000. Banks and insurance companies must report single cash transactions (or multiple smaller cash transactions under aggregation rules) of $10,000 or more. As part of structuring deposits, the launderer will often use several bank accounts or several life/annuity products with several different financial institutions and deposit the large cash amount in smaller amounts in different institutions over a period of time.

**LAYERING**

The second stage of money laundering involves making the tracing of the illicit funds harder by engaging in several financial transactions. Layering may involve several bank-to-bank or bank-to-insurance company transfers or wire transfers between different accounts in different names. Sometimes layering will involve financial institutions in different countries and changing from one currency to another. Another way to change the form of the funds once they are in the financial system is to purchase high value items such as art, jewelry or diamonds. Layering is usually the most complicated stage in the money laundering process and is undertaken to make the original illicit money as hard to trace as possible.

**INTEGRATION**

In the last stage of money laundering, integration, the laundered funds re-enter the economy, appearing legitimate since they arrive from legitimate sources (such as a check from an insurance company). Integration can involve the surrendering of life insurance policies or annuities purchased with illicit funds. Integration may involve the criminal investing laundered funds in a legitimate business, the purchase of assets such as real
estate or securities, or the sale of high value items that were purchased during the layering stage. Integration sometimes utilizes fake companies (shell companies) that exist for no reason other than to launder money. These fake companies take in money as payment for fictitious goods and services but never provide the goods or services; they simply create the appearance of a legitimate business through fake invoices and financial statements. After integration the criminal can usually use the laundered funds with little fear of getting caught if there was no documentation during the two previous stages.

**HOW TERRORIST FINANCING DIFFERS FROM TRADITIONAL MONEY LAUNDERING**

The financing of terrorists involves all three stages of money laundering, except that during integration the object is to distribute the funds to terrorists and their supporting organizations, which is a criminal activity.

These three stages of money laundering may occur as separate and distinct phases, they may occur simultaneously or, more commonly, they may overlap. How the basic steps are carried out depends on the laundering mechanisms used and the requirements of the criminal.
Section 1 - Review Questions

1. Which of the following insurance products are NOT considered "covered products" under the anti-money laundering regulations?
   (a) Property & Casualty insurance
   (b) Annuities
   (c) An insurance product with ability to store value that can be transferred
   (d) Whole life insurance

2. Injecting illicit funds into the financial system through transactions such as the purchase of an annuity is an example of which stage of money laundering?
   (a) Integration
   (b) Structuring
   (c) Layering
   (d) Placement

3. For the purposes of anti-money laundering efforts, the terms “cash” or “cash equivalents” includes all of the following EXCEPT:
   (a) Currency
   (b) A check drawn on the customer’s account
   (c) A traveler’s check
   (d) A money order

4. Which of the following statements best describes “money laundering”?
   (a) The process by which funds from outside the United States enter the U.S. economy.
   (b) A two step process undertaken by criminals to evade taxes.
   (c) Using financial transactions to conceal the identity, source, and/or destination of illegally gained money, by which the proceeds of crime are converted into assets which appear to have a legitimate origin
   (d) Laundering money.

5. Insurance companies are required to file Suspicious Activity Reports with:
   (a) The IRS
   (b) The Financial Crimes Enforcement Network
   (c) The State Insurance Commissioner
   (d) Their annual financial statements

6. Surrendering a whole life policy purchased with illicit funds is an example of:
7. The intent of the USA Patriot Act is:

(a) To ensure that all criminals pay the appropriate tax on illicit funds.
(b) To identify and track terrorist and persons or entities using U.S. financial institutions to further their causes and to prevent money laundering by terrorists or other criminal organizations.
(c) To identify unsuitable sales to seniors within the financial services industry.
(d) To protect U.S. based businesses against unfair competition from abroad.

8. The three basic stages of money laundering:

(a) Are always separate and distinct.
(b) Never overlap.
(c) Must be undertaken in a specific order to be considered money laundering.
(d) May occur simultaneously or overlap.

9. Which of the following transactions below is most likely to be considered layering?

(a) The breaking of large illicit cash deposits into several smaller deposits.
(b) Using illicit cash to buy an annuity.
(c) Transferring illicit funds from bank-to-bank or bank-to-insurance company.
(d) Taking the maximum loan against a whole life policy.

10. Breaking a large cash deposit amount into several smaller deposits is an example of:

(a) Structuring deposits
(b) layering
(c) Integration
(d) Tax evasion
Section 2

AML Rules & Regulations

USA PATRIOT ACT TITLE IIII

The USA Patriot Act Title III Regulations became effective May 2, 2006. On this date insurance companies were required to have AML programs in place.

The Sections of The USA Patriot Act that directly affect insurance companies are contained in sections 326 and 352. These sections require each insurance company to develop and implement a board-approved, written program that applies to Covered Products and is reasonably designed to prevent the insurance company from being used to facilitate money laundering or terrorist financing.

SECTION 326 OF USA PATRIOT ACT TITLE IIII

Section 326 mandates that covered insurance companies meet certain requirements related to customer identity, identity verification, customer screening, and records retention. These requirements can be collectively grouped under the heading of Know Your Customer (KYC).

In broad terms, Section 326 mandates that insurance companies:

- Create a Customer Identification Program (CIP).
- Develop and implement Identity Verification (IDV) policies and procedures to ensure that the true customer identity is known.
- Retain Records of information used during customer identity verification. These records must be reasonably accessible.
- Consult the list of suspected and known terrorist (SDN) maintained by OFAC to ascertain if customers are on this list.

SECTION 352 OF USA PATRIOT ACT TITLE IIII

AML PROGRAMS MUST BE

In addition to the establishment of AML programs, Section 352 of the USA Patriot Act requires that as part of the AML program insurance companies:

- Designate an AML Compliance Officer.
• Develop risk-based policies, procedures and controls to identify money laundering.
• Integrate insurance agents into their AML programs.
• Establish an AML training program and provide ongoing training.
• Create an independent audit function to test and verify the effectiveness of the AML program.

Agents and brokers are expected to collect and retain information to help assess the risk associated with particular business transactions. Risk assessment can be categorized into several areas such as:

• Customers in high-risk locations.
• Customers in high-risk businesses or occupations or with high-risk affiliations.
• Insurance products that may be more susceptible to abuse in money laundering activities.

**Examples of High-risk Customers**

Examples of potential high-risk customers that are worthy of additional scrutiny are:

• A senior official in the executive, legislative, administrative, or judicial branch of a foreign government.
• A senior official of a major foreign political party.
• A senior executive of a foreign-owned corporation.
• Any resident of a country that is listed on the “Non Cooperative Jurisdictions” list maintained by the Financial Actions Task Force (FATF).

**Examples of High-risk Businesses**

The U.S. Treasury Department has identified certain types of businesses that may lend themselves to money laundering and may warrant additional scrutiny.

• Offshore corporations and banks or businesses located in high-risk foreign countries (Non Cooperative Jurisdictions).
• Import/export companies.
• Pawn brokers and deposit brokers.
• A jeweler or precious metals dealer.
• Professional service providers such as lawyers and accountants.
• Any cash intensive business such as restaurants, bars, retail stores, convenience stores, strip clubs and parking garages.
• Check cashing facilities.
• Currency exchange houses.

Insurance companies are not prohibited from doing business with high-risk individuals or businesses, but when transacting business there should be enhanced scrutiny and due diligence.

**REPORTING OF SUSPICIOUS ACTIVITY**

Section 352 also requires insurance companies to:

• File reports of suspicious activity using a Suspicious Activity Report (SAR)
• Implement policies and procedures to obtain information from agents, brokers, and employees necessary to detect and report suspicious activity.
• Make policy decisions related to their AML program such as methods of payment acceptance and approval levels and processes for certain transactions.

While all insurance companies must follow the same regulations to comply with the AML laws, their AML programs can vary due to the types of covered products they sell, methods of product distribution and geographic area served. Therefore, it is important that the agent become familiar with the AML program of the insurer(s) they represent.
Section 2 - Review Questions

1. Which of the following is NOT an example of a high-risk business?

   (a) A Pawn broker
   (b) An offshore corporation
   (c) An import/export company
   (d) A commercial building contractor

2. Which of the following is NOT a requirement for an insurance company AML program?

   (a) An AML Compliance officer must be designated
   (b) Integrate agents into the program
   (c) Develop risk-based policies and procedures
   (d) Track insurance agent commissions

3. Which of the following would be considered a high-risk customer?

   (a) A senior official in the judicial branch of a foreign government
   (b) A senior official of a U.S. political party
   (c) A senior official of a U.S. Corporation
   (d) The treasurer of a local city government
Section 3
Agent & Broker Responsibilities Under AML Regulations

One of many elements of the USA Patriot Act requires insurance companies to establish AML programs and for the Treasury Department to set standards for these programs.

The Treasury Department and its Financial Crimes Enforcement Network (FinCEN) have issued regulations requiring insurance companies to establish AML programs that meet certain minimum standards and also to report suspicious transactions. The Treasury department and FinCEN have stated that insurance agents and brokers are expected to play an important role in the AML programs.

As part of the minimum standards required in the AML law, insurance companies are required to integrate agents into their AML programs and monitor their compliance.

The preamble to these rules states that if efforts to integrate agents into insurance company AML programs are not effective, FinCEN may begin requiring agents to establish their own AML programs.

Life insurance agents often have direct contact with the customers and are often best positioned to gather information and detect suspicious activity.

**GAIN FAMILIARITY WITH COMPANY AML PROGRAMS**

As part of their AML program each insurer will require their agents to complete AML training on an ongoing basis. Many insurance companies have periodic training on their specific policies and procedures that are part of their AML program.

**PAYMENT METHODS**

One area where many company AML programs will differ is which methods of payments will be accepted. In addition to limiting accepted methods of payment, some insurance companies will place dollar limits on certain types of transactions that may be accepted without management approval.

When an insurance company addresses accepted methods of payment as part of an overall AML program, the goal is to reduce the chances that the insurance business will be involved in money laundering without excluding forms of payment with a legitimate business purpose. Because agents and brokers often collect at least the first premium due under a policy, they may be called upon to inform customers of these standards and to
enforce them.

Obviously, the agent should be very familiar with the insurance company payment acceptance policy to prevent the acceptance of a payment type or amount outside the bounds allowed by the insurance company’s AML program.

Below are three partial examples of payment method requirements included in insurance company AML programs.

**PAYMENT METHODS EXAMPLE 1**

- The insurance company will not accept currency (cash) as a form of payment.
- The insurance company prohibits agents who sell its products from accepting cash from a client and converting this cash to another form of payment (e.g. personal check, company check, money order, traveler’s check, etc.) that will be remitted to the insurance company.
- The insurance company restricts the acceptance of money orders or traveler’s checks to $1,000 per day per client. The insurance company has determined that these types of payments have a higher level of risk of money laundering, and has therefore restricted their use.

**PAYMENT METHODS EXAMPLE 2**

- The insurance company and agents of the insurance company are prohibited from accepting payments in the form of cash, traveler’s checks, third party checks, checks drawn on foreign financial institutions, payments in foreign currency, and wire transfers from foreign institutions.

**PAYMENT METHODS EXAMPLE 3**

Only the following will be accepted:

- Personal or business checks payable only to the insurance company with the full name and address of the payor.
- Transfers from trust accounts.
- Payments from insurance companies whose policies are exchanged for a policy with insurance company receiving the premium payment.
- Electronic Funds Transfer drawn from the policy owner or payor’s bank account.
- Wire Transfers to the insurance company’s account from an American Bank.
- Money orders under $5,000, and/or Cashiers Checks, Bank Drafts, Bank Checks, Treasurer’s Checks over $10,000.
• Cash equivalents between $5,000 and $10,000 will be accepted if there is a legitimate business reason for the use of such cash equivalents. Legitimate business reasons have been determined in advance and can also be looked at on a case-by-case basis.

• Third Party Checks will be accepted on a case-by-case basis, based on a legitimate business need.

**RED FLAGS CAN ALERT AN AGENT TO SUSPICIOUS ACTIVITY**

There are certain red flags that can alert an agent to a suspicious transaction or activity. As a first line of defense in the insurance company’s fight against money laundering and terrorist financing, it is critical that the agent develop the ability to recognize red flags that may indicate attempts to launder money or finance terrorism.

It is important for the agent to be aware that their role in connection with the customer often places them in the best position to observe suspicious behavior. The agent should remain alert for suspicious behavior at all times during their relationship with the customer, not just during the initial contact and transaction.

If the agent detects suspicious behavior, they should follow the directions for reporting suspicious activity described in the insurance company AML program. This usually involves communicating with the designated AML compliance officer identified in the insurance company AML program.

**NOTE:** The insurance company may be required to file a Suspicious Activity Report (SAR) with the U.S. Department of the Treasury.

The agent MUST NOT, under any circumstances, disclose the fact that a SAR has been filed or considered, or the contents of a SAR, to the subject or to any third party.

It is a federal crime to disclose reportable information to the customer or any other unauthorized party.

**PARTIAL LIST OF RED FLAGS**

Whether an activity is suspicious or not will depend upon the type of activity, and the customer's normal activity. Generally, transactions that appear to lack a reasonable economic basis or recognizable strategy should be reported as suspicious. Other things to look for include:

• Any transaction involving an undisclosed party.

• Customers who attempt to violate the insurance company payment restrictions by
structuring certain types of payments over time, or request the agent’s assistance in doing so.

- The payment of a large amount broken into smaller separate amounts (structuring).
- Customers who intend to fund policies or contracts via unrelated third parties, other than rollovers from other financial institutions.
- The purchase or funding of a product that appears to exceed a customer’s known income or liquid net worth.
- The purchase of a product that appears to be inconsistent with a customer’s needs.
- A dramatic change in the pattern of business activities.
- Excessive cash or currency transactions where checks are normally used.
- Customer pays premium using foreign currency or lump-sum wire transfer.
- Payments to or from unknown third parties.
- Use of a "third party check" to pay for a policy.
- Customer makes a substantial overpayment of the premium, then asks for a refund.
- Application for a policy from a potential client in a distant place where a comparable policy could be provided closer to home.
- Customer is indifferent about product details and information normally of interest to a person purchasing such a plan (ie: performance, fees, loads, surrender charges).
- Customer shows little or no concern for the investment performance of an insurance product, but much concern about the early termination features of the product.
- Unusual early redemptions of insurance or annuity contracts without regard for penalties or fees.
- Request that a recently purchased policy be surrendered or “not taken” with payment requested to go to a third party.
- A “not taken” policy termination after initial premium included payment of cash equivalent.
- Customer use of life insurance policies for revolving loans paid back quickly with cash equivalents.
- Customer wants to borrow the maximum cash value of a single premium life insurance policy, soon after paying for the life insurance policy.
- Customer appears to have life insurance policies with several institutions.
- Customer resists providing information related to their identity, the source of funds, or the intended use of the policy or contract, or provides information that is
• Incomplete information, excessive secrecy (what do you need to know that for?), or delay in information needed to verify identity.
• Customer request a change of ownership to a foreign national.
• Customer directs proceeds on claims or other disbursements to third parties in foreign countries.
• The use of P.O. boxes, C/Os, or agent address as owner addresses.
• The customer attempts to sell a life insurance policy in a viatical settlement transaction soon after purchase or expiration of the incontestability period.
• The customer has difficulty describing the nature of his or her business or lacks general knowledge of their stated industry.

**KNOW YOUR CUSTOMER (KYC)**

The AML laws require insurance companies to collect customer information from agents and other sources to be used in the Customer Identification Program (CIP) and Identity Verification (TDV) process. The insurance company also must retain the records in a reasonably accessible manner.

Under the Know Your Customer guidelines, the agent must collect and verify identifying information about each customer.

**INFORMATION REQUIRED FOR CUSTOMER IDENTIFICATION**

There are a minimum of four specific pieces of information that the agent must obtain for each customer.

• Name
• Date of Birth
• Physical Address (not a P.O. Box, commercial mailbox, or company address)
• Social Security or Tax ID #

Verification of this information must be done through use of a photo ID such as a driver's license or other government issued picture ID document. **Verification through use of documents without a photo ID is insufficient.**

**ACCEPTABLE DOCUMENTS FOR IDENTIFICATION OF AN INDIVIDUAL**

Only certain documents are acceptable for customer identification. For individuals the photo identification should consist of one or more of the documents below.
• Driver’s license (issued by a state or territory of the United States)
• U.S. Passport
• State-issued photo ID (usually where someone does not have a state-issued driver’s license)
• U.S. Military ID
• Resident Alien card (green card)
• Foreign Government ID card (resident or non-resident alien)

The agent is not required under the AML laws to retain a photocopy of the individual’s identifying document, but should physically look at the card and not take this information over the phone.

**NOTE: Some insurance companies DO require the agent to retain a copy of the individual’s identification document.**

**ACCEPTABLE DOCUMENTS FOR IDENTIFICATION OF A BUSINESS ENTITY**

For business entities the identification document should consist of one of the documents listed below depending on the type of business entity. If the agent is unfamiliar with the documents listed below they should ask for guidance from management within the insurance company:

• Certified Articles of Incorporation (for corporations)
• LLC Operating Agreement (for LLC and LLP entities)
• Partnership Agreement (for general partnerships)
• Organizing Documents (many insurance companies have an additional level of review for these documents)
• Trust Documents
• Certified Financial Statements
• Certificate of Good Standing issued by a government authority
• A government-issued Business License

**NON-DOCUMENTARY IDENTITY VERIFICATION**

If the agent is conducting business over the phone, via mail, online, or the customer is applying for a policy on behalf of an individual the agent does not meet, the identity of
the customer can be verified by the insurance company using other methods. This is called a Non-Documentary method of identity verification.

Some insurance companies on a risk-based approach will use non-documentary methods of identity verification in addition to verification of identity through a photo ID for some customers.

Generally, non-documentary identity verification can be achieved using one or more of the methods below:

- Comparing the information gathered with data available from a third party such as a credit bureau, or government website.
- Contacting the client after the account is opened to verify that address, phone numbers, and social security numbers are valid.
- Physically visiting a site to verify the existence of a client's residence or place of business.
- Comparing the information provided by the client against fraud and bad check databases.
- Checking references with other financial institutions.

The AML laws do not require the insurance company to take steps to determine whether the document that the customer has provided for identity verification has been validly issued and the insurance company may rely on a government-issued identification as verification of a customer’s identity. However, if the insurance company notes that the document shows some obvious form of fraud, they must consider that factor in determining whether they can form a reasonable belief that they know the customer’s true identity.
Section 3 - Review Questions

1. Which of the following is most likely to NOT be an acceptable form of payment with an insurance company?

(a) Money Order
(b) Cash
(c) Traveler’s Check
(d) Wire transfer for a U.S. bank

2. Which of the following is NOT an acceptable form of identification for an individual?

(a) Drivers license issued by a state or territory of the United States
(b) Voter card issued by a foreign government
(c) U.S. Passport
(d) U.S. Military ID

3. If you are doing business with an individual over the phone and do not meet them in person:

(a) Their identity cannot be verified.
(b) You must report the contact as suspicious activity.
(c) The insurance company may be able to verify their identity though non documentary methods.
(d) You can take their photo ID information over the phone.

4. Which of the following would NOT be considered suspicious activity?

(a) A “not taken” when the initial premium payment was made via a money order for $4,900.
(b) The customer makes several loans from a life policy and immediately repays them with cash equivalents.
(c) The customer request a loan on a single premium life policy sold 5 years ago where the initial premium was paid by personal check from the customer.
(d) The customer resists providing information relating to identity.
Section 4

Reporting Suspicious Activity and Consequences for Non-Compliance

IDENTIFICATION AND REPORTING OF SUSPICIOUS ACTIVITY

Insurance agents are not required by the AML laws to have separate anti-money laundering programs. However, insurance agents and brokers are an integral part of the insurance industry due to their contact with customers. Insurance agents are typically involved in sales operations and are, therefore, in direct contact with customers. As a result, the agent will often be in a critical position of knowledge as to the source of investment assets, the nature of the clients, and the objectives for which the insurance products are being purchased.

Agents have an important role to play in assisting the insurance company to prevent money laundering. Therefore, the AML laws require each insurance company to integrate its agents into its anti-money laundering program and to monitor their compliance with its program. The AML laws also require an insurance company’s anti-money laundering program to include procedures for obtaining relevant customer-related information necessary for an effective program, either from its agents or otherwise.

Although under the AML laws, insurance agents are not independently required to report suspicious transactions, the same laws make clear that agents are expected to work with insurance companies in identifying suspicious transactions that the insurance company must report.

INSURANCE AGENTS CONTRACTUALLY OBLIGATED TO REPORT SUSPICIOUS ACTIVITY

During the rule-making process, FinCEN expected that companies would use their contractual relationships to require agents to provide them with information that may be useful for identifying potential suspicious activity.

The contractual responsibilities of agents with respect to anti-money laundering programs are similar to the responsibilities agents undertake in connection with company customer identification and anti-fraud procedures. Insurers already have compliance and best-practices guidelines that both captive and independent agents follow in order to continue doing business with them. Insurers also require very extensive information-gathering by many of their agents for underwriting purposes. Many insurance companies have adopted the same structural model for their anti-money laundering programs.

Most insurance companies require the agent to immediately refer any suspicious activity to their designated AML compliance officer. The agent should be alert to suspicious activity at all times, not just during the initial customer transaction. If an agent suspects there is a potential for money laundering, they should immediately contact the AML compliance officer and await instructions.
The agent should never attempt to investigate the suspicious activity on their own.

Since the insurance company must report the suspicious activity to the U.S. Treasury within 30 days of identification, the agent should not delay referring the information to the AML compliance officer, who will determine if the suspicious activity warrants filing a SAR.

**REQUIRED REPORTING OF SUSPICIOUS TRANSACTIONS**

Insurance companies are required to report suspicious transactions that are conducted or attempted by, at, or through the insurance company and that involve an aggregate of at least $5,000 in funds or other assets (not limited to currency). A transaction is suspicious if the insurance company knows, suspects, or has reason to suspect that the transaction or pattern of transactions:

- Involve funds derived from illegal activity or are intended to hide funds derived from illegal activity,
- Are designed to evade reporting requirements imposed by Federal law,
- Have no apparent lawful purpose or are not the sort in which a particular customer would be expected to engage, or
- Involve the use of the insurance company to facilitate criminal activity.

**VOLUNTARY REPORTING OF SUSPICIOUS TRANSACTIONS**

While insurance companies are required to report suspicious transactions that meet the above criteria, they may also voluntarily report transactions as suspicious even if they do not meet the criteria for required reporting.

**REQUIRED REPORTING OF CASH TRANSACTIONS OVER $10,000**

In addition to reporting suspicious transactions, insurance companies are required to report cash transactions in excess of $10,000. For purposes of reaching this $10,000 threshold, multiple currency transactions that take place on the same day, to the same account, for the same person are counted as a single transaction. This is known as the Aggregation Rule. In simple terms, if you have a client who pays more than $10,000 in cash in a single day for a life insurance or annuity product, you should notify the compliance officer of your insurance carrier. The insurance carrier may be required to report this transaction to the IRS.

It may be appropriate for an insurance company to file a Form 8300 for receipt of cash and other items over $10,000 and also file a Suspicious Activity Report when the circumstances surrounding the receipt of cash and other items are suspicious.
PROTECTION FROM LIABILITY FOR REPORTING ACTIVITY AS SUSPICIOUS

Under federal law, insurance agents and insurance companies are protected from liability to customers for disclosing possible criminal activity to their insurance companies, law enforcement, and certain government supervisory agencies. Suspicious Activity Reports and the fact that they have been filed must be kept confidential. In particular, customers cannot be notified that a suspicious activity has been reported.

RECORD KEEPING REQUIREMENTS

The AML laws require the insurance company to maintain records of suspicious transactions for a minimum of 5 years. The records must be readily accessible to regulators. Since suspicious transactions may occur over a period of time before they are identified as such, most insurance companies retain records as long as there is a financial relationship with the customer and 5 years beyond the cessation of the financial relationship.

The agent should also keep copies of any customer information sent to the AML compliance officer.

CONSEQUENCES OF NON-COMPLIANCE

CIVIL PENALTIES

OFAC has levied millions of dollars in civil penalties against U.S. financial institutions, including insurance companies. The majority of fines resulted from the financial institution’s failure to block illicit transfers when there was a reference to a target country, person, or entity, and the SDN list involved in the transaction.

According to OFAC, mitigating factors when considering penalties include self-disclosure to OFAC, the use and sophistication of interdict software, training of employees, AML prevention and detection processes and procedures, and other compliance initiatives.

WILLFUL BLINDNESS

As the term applies to anti-money-laundering efforts, “willful blindness” describes the act of not questioning a transaction when one suspects (or should suspect) that something is amiss. The motivation to engage in “willful blindness” is usually related to money. In the case of a commissioned insurance agent the motivation to engage in “willful blindness” would usually relate to being paid a commission on the transaction if it is executed. An agent can protect themselves and their business from charges of “willful blindness” by reporting any suspicious activity to the AML compliance officer and retaining a copy of the information for your records.
CIVIL PENALTIES

Penalties associated with money laundering are severe. Civil fines may be twice the amount of the transaction, up to $1,000,000. In addition, property involved in the transaction can also be subject to seizure and forfeiture.

Employees and agents of financial institutions can be fined individually and sentenced to imprisonment for up to 20 years for knowing or being willfully blind to the fact that a transaction involves illegal funds.

LOSS OF INSURANCE COMPANY APPOINTMENT

Insurance companies have disciplinary policies and procedures, and an agent who does not fully comply with the company AML policy could be subject to disciplinary action including termination of their contract.

Depending on the situation, the insurance company may also have to report the agent to legal authorities.

DAMAGE TO REPUTATION

Violating anti-money laundering laws could subject the agent and the insurance company to negative publicity, which could cause substantial damage to the professional reputation of the agent and the insurance company.
Section 4 - Review Questions

1. Insurance companies are required to report suspicious transactions that individually or in aggregate total _______.
   (a) more than $10,000
   (b) $5,000
   (c) more than $5,000
   (d) more than $5,000 in a 24 hour period

2. Insurance companies are required to report all cash transactions:
   (a) of $5,000 or more
   (b) of $5,000 or more in a 24 hour period
   (c) of more than $10,000 in a 24 hour period
   (d) as suspicious activity

3. Employees and agents of financial institutions can be fined individually and sentenced to ___________ for knowing or being willfully blind to the fact that a transaction involves illegal funds.
   (a) imprisonment of up to 20 years
   (b) up to 1,000 hours of community service
   (c) up to 5 years of probation
   (d) agents and employees of financial institutions are immune from prosecution under money laundering laws