Anti-Money Laundering for Insurance, 2nd Edition
Course 79_2

RegEd Inc.
2100 Gateway Centre Boulevard, Suite 200
Morrisville, North Carolina 27560
800.334.8322
email: info@reged.com

RegEd Inc. has provided timely and accurate information in the creation of these materials. However, future tax and legal provisions may affect content. These materials do not substitute for legal advice, which may be rendered only by an attorney.

To the extent any RegEd Inc. materials deal with rulings governing the advertisement of life insurance, annuity contracts, accident and health insurance, every effort has been made to ensure the materials presented conform to the New York State Administrative code, specifically Regulations 34 and 34A. However, RegEd Inc. makes no warranty as to this fact, either expressed or implied.

We have designed this course to help you get the most out of your online learning experience. If you have ordered Insurance CE credits with this course, specific rules have been built in to ensure you meet the requirements. These rules will vary depending on the state or designation you selected.

Printed in the United States of America
RegEd.com Product Number: 79.01.01

RegEd

INTRODUCTION

Money laundering is a term used to identify a range of financial transactions designed to conceal one or more of the following with respect to money:

- Its identity;
- Its source;
- Its destination.

It is the process of conducting financial transactions—which may be otherwise legitimate—with money derived from illegitimate sources in order to "cleanse" the money of its taint of illegitimacy. The goal of the money launderer is to be able to eventually spend money derived from illegal activities without drawing attention from where it came.

Money laundering poses a significant threat to the integrity of the financial system and the country's security. Terrorists, drug dealers, arms dealers, and organized crime all have money-laundering needs, and to the extent these criminal elements can get away with it, their illegal activities are encouraged.

Recognizing the threat posed by money laundering, Congress passed a number of laws to prevent money laundering including the USA PATRIOT Act. The Treasury Department required that as of May 2, 2006 life insurance companies had to implement AML programs.

After completing this course, you should be able to do the following:

- *Define money laundering and explain why it is a threat;*
- *Discuss the various anti-money laundering laws including the USA PATRIOT Act;*
- *Explain the implications of anti-money laundering laws and regulations for the life insurance industry;*
- *Discuss the role of the various regulatory agencies that are responsible for anti-money laundering; and*
- *Describe penalties and sanctions for non-compliance with AML laws and regulations.*

MONEY LAUNDERING AND ITS IMPLICATIONS

Money laundering is the process of filtering the proceeds derived from illegitimate criminal activities through one or more legitimate financial transactions. The goal is to place funds from illegitimate activities into the legitimate financial system without attracting attention to the source.

A straightforward example of money laundering involves the drug dealer who receives cash from the sale of controlled substances. The drug dealer deposits the cash in a legitimate bank account. The sales proceeds may be further laundered by investment in a legitimate business enterprise. On the surface, both the cash in the bank account and the cash derived from the business appear perfectly legal. A look behind the scenes reveals both are tainted due to their source.

In this section we will discuss the impacts of money laundering and why it is important to combat money laundering.

1.1 Impact of Money Laundering

In the absence of effective enforcement against money laundering, society is exposed to several threats.

First, if money from criminal activities including drug dealing, counterfeiting, and gambling can be easily diverted to apparently legitimate businesses, the underlying criminal activities are facilitated.

Countries that fail to prevent or curb money laundering are likely to suffer from the social ills of addiction, theft, and violence.

Second, if money laundering is allowed to run rampant, businesses started with funds derived from illegitimate sources compete with legitimate businesses. Because the cost of capital is less for these illegitimate offspring, they have an unfair market advantage over legitimate enterprises and will eventually force them out of business. Further, foreign trade is likely to be curtailed for countries that are

havens for money launderers.

Other countries can be expected to enact protectionist legislation that favors their legitimate domestic businesses over those started by foreign money launderers.

Finally, lack of anti-money laundering laws or lax enforcement of existing laws paves the way for dangerous activities that go beyond ordinary criminal acts. Money derived through money laundering has been used to train and arm terrorists, purchase weapons of mass destruction, and fund terrorist acts.

Because money launderers use financial institutions to help them hide or disguise the proceeds of illicit activities, employees or agents of financial institutions are the first lines of defense against money laundering schemes.

1.2 Crimes that Give Rise to Money Laundering

We've already mentioned some of the illegal activities that give rise to money laundering. The following is a more complete, although not exhaustive, list of the more common illegal activities that lend themselves to money laundering:

- Narcotics transactions;
- Bank fraud;
- Acts of terrorism;
- Copyright infringement or counterfeiting;
- Violations of the U.S. economic sanctions laws;
- Smuggling or theft;
- Misapplication of funds by a bank officer or employee;
- Embezzlement;
- Illegal avoidance of federal tax payments;
- Murder; and
- Illegal dumping.

An important point to keep in mind is at least some of these activities are the work of a sophisticated criminal mind. Crimes that give rise to money laundering are not committed only by people who look like we expect criminals to look. They are also committed by corporations, large and small, and white-collar executives.

1.3 Common Transactions Used to Launder Money

Money may be laundered through a variety of transactions. The simplest case involves the deposit of illegitimately obtained funds into a legitimate financial

vehicle such as a bank account, cash value life insurance policy, or annuity. But money launderers are creative and have been known to use all of the following financial vehicles in an effort to cleanse funds:

- Cash deposits and withdrawals;
- Wire transfers and electronic funds transfers;
- Money orders, cashier's checks, and travelers' checks;
- ATM debit cards and credit cards;
- Letters of credit; and
- Loans.

What all of these have in common is they facilitate the movement of funds from one arena to another. Anytime funds are shifted, there is potential for money laundering.

Irrespective of the original source of the illegally-derived funds, money laundering follows a common pattern involving three stages, known as:

- *Placement:* the point at which illegally-derived funds enter the financial system via investment in a brokerage account, deposit into a savings vehicle, etc.;
- *Layering:* the movement of funds through transactions within the financial system designed to obscure the link between the source of the funds and their return to the legitimate economy; and
- *Integration:* the re-entry of the "laundered" funds into the economy for possible use in the funding of illegal and/or terrorist acts.

1.4 Summary

Money laundering is the process of filtering the proceeds derived from illegitimate criminal activities through one or more legitimate financial transactions. Money laundering is problematic because:

- It facilitates illegal activities.
- It provides businesses started with laundered funds with an unfair competitive advantage over legitimate businesses.
- It paves the way for dangerous activities that go beyond ordinary criminal acts.

A wide variety of criminal activities generate funds that are often the source of money laundering. A wide variety of legitimate transactions can be used to launder funds garnered through illegitimate sources.

1. The process of conducting legitimate transactions with money derived from illegitimate sources for the purposes of cleansing it is called what?

A. Illegitimate dealings **Your answer is incorrect. The correct reference is not "illegitimate dealings".**
B. Embezzlement **Your answer is incorrect. The correct reference is not "embezzlement".**
C. Cleaning **Your answer is incorrect. The correct reference is not "cleaning".**
D. Money laundering **Your answer is correct. Money laundering is the process of conducting legitimate transactions with money derived from illegitimate sources in order to "cleanse" the money of its taint of illegitimacy. The goal of the money launderer is to be able to spend money derived from illegal activities without drawing attention.**

2. When were all insurance companies required to comply with the USA PATRIOT ACT?

A. May 2006 **Your answer is correct. Congress has passed a number of laws to prevent money laundering, including the USA PATRIOT Act. The Treasury Department indicated that beginning in May 2006, life insurance companies not already subject to the USA PATRIOT ACT had to comply with its anti-money laundering provisions.**
B. October 2001 **Your answer is incorrect. It was not October 2001.**
C. October 2005 **Your answer is incorrect. It was not October 2005.**
D. April 2003 **Your answer is incorrect. It was not April 2003.**

3. Who are the most likely to participate and benefit in money laundering activities?

I. Bankers
II. Terrorists
III. Lawyers
IV. Drug Dealers

A. I and II **Your answer is only partially correct.**
B. II and IV **Your answer is correct. Terrorists and drug dealers are the most likely to participate and benefit in money laundering activities.**
C. II and III **Your answer is only partially correct.**

D. I and III **Your answer is incorrect. Bankers and lawyers are not the most likely to participate and benefit in money laundering activities.**

MONEY LAUNDERING CONTROL ACT OF 1986

There are three major laws that are relied on in the prevention of money laundering:

- *Money Laundering Control Act of 1986 (MLCA)*
- *Bank Secrecy Act*
- *USA PATRIOT Act*

This section focuses on the MLCA.

1.5 Scope of Money Laundering Control Act

The Money Laundering Control Act of 1986 (MLCA) was the first federal law to define money laundering and designate it as a crime. Under the MLCA there are three categories of money laundering violations.

- Financial transaction money laundering
- Transportation money laundering
- Monetary transaction money laundering

Although this course focuses only on the federal crime of money laundering, it is important to note most states also make money laundering a crime.

1.6 Financial Transaction Money Laundering

Under the MLCA, 18 U.S.C. Section 1956 (a) (1) four types of financial transaction money laundering crimes are identified.

Like most crimes, the burden is on the prosecution to not only prove that the accused committed certain specified acts, but that the acts were performed with a prohibited state of mind.

With **financial transaction money laundering** the prohibited action is conducting or attempting to conduct a financial transaction, knowing that the money or other property involved represents the proceeds of some form of unlawful activity.

The prohibited state of mind is:

- The intent to promote a specified unlawful activity;
- The intent to illegally avoid (or assist in the avoidance of) the payment of federal income taxes;
- Knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity; or
- Knowing that the transaction is designed in whole or in part to avoid a transaction reporting requirement under State or Federal law.

For purposes of the MLCA a **specified unlawful activity** is any one of the 200 designated crimes specified in the act including crimes such as illegal drug trafficking, fraud, and counterfeiting.

Any person engaging in the prohibited action with the requisite state of mind is guilty of one or more of the crimes of financial transaction money laundering.


Example

Lars, a commercial loan officer, takes advantage of his position to approve bank loans to sham corporations that he establishes; he redeposits the stolen funds in business checking accounts.

Anyone guilty of any of these crimes may be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than 20 years, or both.

1.7 Transportation Money Laundering

Transportation money laundering crimes are described in 18 U.S.C. Section 1956 (a) (2).

Under this section of the statute, the prohibited act is the transportation, transmission, transfer, or attempted transportation, transmission, or transfer of a monetary instrument or funds from a place in the United States to or through a place outside the United States, or to a place in the United States from or through a place outside the United States.

To be convicted of transportation money laundering, the prosecution must show the defendant committed the act:

- With the intent to promote specified unlawful activity;

- Knowing the monetary instrument or funds involved in the transportation, transmission, or transfer represent the proceeds of some form of unlawful activity and knowing that such transportation, transmission, or transfer is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activity; or
- To avoid a transaction reporting requirement under State or Federal law.


Example

Weasel runs a methamphetamine lab from his home in New York and sells the product on the street through a network of underage boys. Once a week he wire-transfers a portion of his funds to his brother's checking account in Los Angeles. Weasel's brother invests the funds in legitimate mutual funds. Weasel has probably engaged in transportation money laundering.

Transportation money laundering crimes carry a fine of not more than $500,000, or twice the value of the monetary instrument or funds involved in the transportation, transmission, or transfer, whichever is greater, or imprisonment for up to 20 years, or both.

1.8 Monetary Transaction Money Laundering

Monetary transaction money laundering involves engaging or attempting to engage in a monetary transaction in criminally derived property of a value greater than $10,000 where the property is derived from specified unlawful activity.


Example

Carter regularly travels to Mexico for the purpose of importing marijuana for sale here in the states. He uses a portion of the funds in excess of $10,000 to purchase a new automobile to make his travel more comfortable. Carter has probably engaged in monetary transaction money laundering.

A guilty party may be fined up to twice the amount of the criminally derived property involved in the transaction, and may face imprisonment of up to ten years, or both.

1.9 Summary

- The Money Laundering Control Act of 1986 (MLCA) defines and designates money laundering as a crime.
- Under the Act there are three types of money laundering:
  - Financial transaction money laundering
  - Transportation money laundering
  - Monetary transaction money laundering

- In addition, most states have similar laws making money laundering a crime.

1. Failure to enforce anti-money laundering laws allows businesses started with illegitimate sources to compete with what businesses?

A. American **Your answer is incorrect. American businesses is not the most accurate reply.**
B. Banking **Your answer is incorrect. Banking businesses is not the most accurate reply.**
C. Legitimate **Your answer is correct. If money laundering is allowed to run rampant, businesses started with funds derived from illegitimate sources compete with legitimate businesses. Because the cost of capital is less for these illegitimate offspring, they have an unfair market advantage over legitimate enterprises and will eventually force them out of business. Furthermore, foreign trade is likely to be curtailed for countries that are havens for money launderers.**
D. Insurance **Your answer is incorrect. Insurance business is not the most accurate reply.**

2. Which of the following are some of the more common activities that lead to money laundering?

I. Smuggling or theft
II. Embezzlement
III. Illegal dumping
IV. Bank fraud

A. I only **Your answer is only partially correct.**
B. II only **Your answer is only partially correct.**
C. III and IV only **Your answer is only partially correct.**
D. I, II, III and IV **Your answer is correct. The following is a more complete, although not exhaustive list, of the more common illegal activities that lend themselves to money laundering:**

- **Narcotics transactions;**
- **Bank fraud;**
- **Acts of terrorism;**
- **Copyright infringement or counterfeiting;**
- **Violations of the U.S. economic sanctions laws;**
- **Smuggling or theft;**
- **Misapplication of funds by a bank officer or employee;**
- **Embezzlement;**
- **Illegal avoidance of federal tax payments;**
- **Murder; and**

- **Illegal dumping.**

3. Anytime funds are shifted from one vehicle to another, there is a potential for what?

A. Money laundering **Your answer is correct. Money launderers are creative and have been known to engage in all of the following types of transactions in an effort to cleanse funds**: **cash deposits and withdrawals; wire transfers and electronic fund transfers; money orders, cashier checks and traveler's checks; ATM debit cards and credit cards; letters of credit; and loans. What all of these transactions have in common is that they facilitate the movement of funds from one arena to another. Anytime funds are shifted, there is the potential for money laundering.**
B. Cash movement **Your answer is incorrect. Although shifting funds may indicate "cash movement" it is not the accurate reply.**
C. Embezzlement **Your answer is incorrect. Although shifting funds may indicate "embezzlement" it is not the accurate reply.**
D. Criminal transactions **Your answer is incorrect. Although shifting funds may indicate "criminal transactions" it is not the accurate reply.**

BANK SECRECY ACT

Although enacted four decades ago, the Bank Secrecy Act continues to serve as a key weapon against money launderers.

This section considers the provisions of the Bank Secrecy Act and its implications for financial institutions including life insurance companies and their employees.

1.10 Scope

Congress enacted the **Bank Secrecy Act (BSA)** in 1970. The purpose of the BSA is to prevent banks and other financial services institutions including life insurance companies from being used to hide the transfer or deposit of illegally obtained funds or from being used as intermediaries for this purpose.

Because drug traffickers and terrorists are often engaged in money laundering, the federal government through its enforcement arms in the Department of Justice and Treasury Department also uses the BSA to crack down on drug trafficking and terrorism.

1.11 Currency Transaction Reporting

At the heart of the BSA is a requirement that financial institutions including life insurance companies record and report to the federal government all currency transactions made by any person or entity that total $10,000 in a single day. The required report is referred to as a **Currency Transaction Report.**

Money launderers sometimes attempt to skirt the requirements of the BSA by employing individuals to make several deposits in different locations, with each deposit amounting to less than the $10,000 threshold. This process is also known as **smurfing** and the individuals who make the deposits are called **smurfs.**

1.12 Cross Border Transactions

The BSA also mandates reporting cross-border transports of monetary instruments and of foreign bank accounts. The term **monetary instrument** includes the following:

- Coins;
- Currency;
- Traveler's checks;
- Bearer bonds;
- Securities; and

- Negotiable instruments.

1.13 Additional Legislation

Since its enactment in 1970, Congress has passed several additional laws that compliment, strengthen, or enhance the BSA. The following table summarizes this legislation:

	Legislative Action
1986	Money Laundering Control Act (MLCA) defines and designates money laundering as a federal crime.
1992	Annunzio-Wylie Anti-Money Laundering Act requires the reporting of suspicious activities. It also gives the federal government the power to revoke federal deposit insurance and charters for any financial institution found guilty of engaging in money laundering.
1994	Money Laundering Suppression Act expanded regulators' authority to combat money laundering by requiring "money-transmitting services" to register with the Financial Crimes Enforcement Network (FinCEN) or face a $5,000 penalty.
2001	In response to the 9/11 terrorist attacks Congress enacts the USA PATRIOT Act. This important legislation broadens the definition of financial institution, imposes significant new due diligence and other requirements on financial institutions, increases the powers of the government to impose sanctions for violations, and includes a number of special measures for improving information sharing and cooperation among financial institutions and law enforcement.

FinCEN is an agency of the Treasury Department. It is charged with oversight and implementation of the federal anti-money laundering laws. It passes intelligence to state, federal, and international law enforcement agencies and financial industry regulators to help them in their efforts to combat money laundering.

1.14 Summary

- The BSA imposes reporting requirements on banks and other financial institutions in order to minimize money laundering activities.
- At the heart of the BSA is a requirement that financial institutions file a Currency Transaction Report disclosing all currency transactions made by any person or entity that total $10,000 in a single day.
- The BSA also requires reporting of cross-border transports of monetary instruments and of foreign bank accounts.
- Since the enactment of the BSA in 1970 several other laws have been enacted to broaden and enhance the scope of the BSA. These additional laws include the following:

    - Money Laundering Control Act (MLCA)
    - Annunzio-Wylie Anti-Money Laundering Act
    - Money Laundering Suppression Act
    - USA PATRIOT Act.

1. Which was the first federal law to define money laundering and call it a crime?

A. USA PATRIOT ACT **Your answer is incorrect. USA PATRIOT ACT was not the first federal law to define money laundering and call it a crime.**
B. MLCA **Your answer is correct**. **The Money Laundering Control Act of 1986 (MLCA) was the first federal law to define money laundering and designate it as a crime. Under the MLCA there are three categories of money laundering violations: Financial transaction money laundering; transportation money laundering; and monetary transaction money laundering.**
C. BSA **Your answer is incorrect. BSA was not the first federal law to define money laundering and call it a crime.**
D. AML **Your answer is incorrect. AML was not the first federal law to define money laundering and call it a crime.**

2. How many specified unlawful activities are there in the Money Laundering Control Act?

A. 100 **Your answer is incorrect. One hundred is not the number of specified unlawful activities in the MLCA.**
B. 1000 **Your answer is incorrect. One thousand is not the number of specified unlawful activities in the MLCA.**

C. 200 **Your answer is correct**. **For purposes of the MLCA a specified unlawful activity is any one of the 200 designated crimes specified in the act itself, including crimes such as illegal drug trafficking, fraud, and counterfeiting.**
D. 50 **Your answer is incorrect. Fifty is not the number of specified unlawful activities in the MLCA.**

3. Monetary transaction money laundering involves attempting to engage in a monetary transaction with criminally derived property in excess of $_____.

A. 5000 **Your answer is incorrect. $5000 is not the correct amount.**
B. 1000 **Your answer is incorrect. $1000 is not the correct amount.**
C. 100,000 **Your answer is incorrect. $100,000 is not the correct amount.**
D. 10,000 **Your answer is correct. Monetary transaction money laundering involves engaging in, or attempting to engage in, a monetary transaction in criminally derived property of a value greater than $10,000 where the property is derived from specified unlawful activity.**

The USA PATRIOT Act

Enacted to combat the threat of global terrorism, the USA PATRIOT Act has far-reaching implications for the financial services industry including life insurers.

This section contains an overview of the USA PATRIOT Act, enacted by Congress in October 2001. Upon completing this section, you will be able to do the following:

- *Identify the basic purpose of the USA PATRIOT Act;*
- *Define "financial institution" for purposes of the USA PATRIOT Act;*
- *Explain why life insurance companies are considered financial institutions under the USA PATRIOT Act; and*
- *Describe the application of the USA PATRIOT Act to life insurance companies, agencies, and agents and brokers.*

1.15 Overview

In October 2001, Congress responded to the 9/11 terrorist attacks by enacting wide-ranging legislation intended to make it more difficult for terrorists to carry out their activities. The full title of this important legislation is the **U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act. As you can see, the first letters of each word in the full title of the act spell out the USA PATRIOT Act.

According to the Congressional record the stated purposes of the USA PATRIOT Act is to:

- Deter and punish terrorist acts in the United States and around the world,
- Enhance law enforcement investigatory tools, and
- Strengthen measures for detecting, preventing, and prosecuting money laundering.

Title III of the Act, entitled the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 is most relevant to financial institutions including life insurance companies.

In general, Title III of the USA PATRIOT Act:

- Broadens the definition of the term financial institution for purposes of anti-money laundering compliance;
- Imposes significant due diligence and other requirements on financial institutions;
- Increases the government's forfeiture powers and other sanctions for violations; and
- Includes measures designed to improve information sharing and cooperation between financial institutions and law enforcement.

1.16 Financial Institutions

The USA PATRIOT Act significantly expands the definition of "financial institutions" for purposes of its anti-money laundering provisions. The definition is broad enough that if an entity provides financial services, it must generally comply with the Act’s requirements.

Under the USA PATRIOT Act, "financial institution" is defined to include any business or agency that:

- Employs more than 30 employees;
- Generates annual revenues in excess of $2 million;
- Maintains offices both within and without the United States; and
- Engages in any activity that involves the exchange of funds.

Both the Treasury Department and the life insurance industry through its industry organizations NAIFA and ACLI acknowledge that life insurance companies fall within this definition of financial institution.

The Treasury Department through its agency FinCEN applied anti-money laundering program requirements to insurance companies, as well as SAR filing. Insurers are required to “integrate agents into their anti-money laundering programs.”

Further, the term *financial institution* with respect to insurance companies refers to those insurers issuing "covered products." Property-casualty and health insurance companies to the extent they do not issue covered products are not covered under the law.

1.17 Life Insurance Companies as Financial Institutions

Life insurance products including both cash value life insurance policies and annuity contracts are considered at risk for money laundering because they have investment features similar to bank and other investment products.

The key investment features that place life insurance products at risk for money laundering are:

- Stored value; and
- Transferability.

Stored value refers to the ability of life insurance policies and annuities to accumulate cash values that can be accessed through loans and/or withdrawals and surrenders.

Transferability refers to the fact that life insurance policies and annuities can be transferred and retransferred by the owner to another individual or entity, making it difficult to determine the original source of the funds.

Max, a notorious drug trafficker, hands Irma a large sum of cash derived from his illegal activities. Irma uses the cash to buy single premium deferred annuities with several life insurance companies. To the extent that withdrawals and distributions from the annuities are used to provide for the legitimate needs of Max's children and grandchildren, he has successfully laundered his ill-gotten gains.

1.18 Application of the USA PATRIOT Act to Life Insurance Companies

The final rule governing the application of the USA PATRIOT Act to insurance companies was published in the Federal Register. The final rule prescribes the *minimum standards* that apply to insurance companies under the provisions of the Bank Secrecy Act requiring financial institutions to establish AML programs.

1.18.1 Insurer AML Program Required for "Covered Products"

The final rule concerning the establishment of AML programs by insurance companies does not apply to all insurance companies. Instead, the final rule applies only to insurance companies that offer insurance products termed "covered products." Further, the definition of *insurance company* under the final rule is narrowed to exclude from the provisions of the rule those persons whose issuance of a covered product is only an incidental part of their noninsurance business.

According to the final rule, the term *covered product* means:

- A permanent life insurance policy, other than a group life insurance policy;
- An annuity contract other than a group annuity contract; and
- Any other insurance product with features of cash value or investment.

Applying this definition of "covered product," we can see that any insurance company that issues individual permanent life insurance policies—including universal life insurance—or individual annuity contracts is included in the final rule. However, insurance products other than individual permanent life insurance policies or annuity contracts, including those that may not yet exist, are included in the definition of a covered product insofar as they incorporate similar cash value or investment product features.

An understanding of the rationale behind the inclusion of certain insurance products and the exclusion of others in the final rule is important. The covered insurance products included in the rule are those that possess features that could make them useful to individuals or organizations interested in money laundering or financing terrorism. Clearly, permanent life insurance policies and annuity contracts with their cash surrender values would allow a money launderer to use illegally-derived funds to pay premiums and then take withdrawals or loans—or surrender the policy or contract entirely—to obtain clean, "laundered" funds with which to further illegal or terrorist agendas.

Some insurers issue both covered products and products not considered covered products. Such an insurer is not required to adopt a company-wide AML program applicable to all its products. The final rule's AML requirement applies only to the insurer's covered products.

1.18.2 Certain Insurance Products Excluded

Certain insurance products not containing cash value or investment features—or which don't permit individuals the same kind of control over the policy or contract—are not considered covered products for purposes of the final rule. Insurers issuing *only* these non-covered products would not generally be subject to the rule requiring insurance companies to establish AML programs.

The products *excluded* from the list of covered products under the final rule are those in which the risks of money laundering do not exist to the same degree and include:

- Term life insurance products, including credit life insurance;
- Group life insurance products;
- Group annuities;
- Property and casualty products;
- Title insurance products;
- Health insurance products; and
- Reinsurance or retrocession contracts.

Bearing in mind any product currently excluded could subsequently be deemed a covered product insofar as it was included in the "catch-all" part of the definition of covered product by possessing a cash value or investment feature, the following considerations led to the exclusion of the above products.

Term life insurance was excluded because it normally involves no usable cash value that can be borrowed, withdrawn, or received upon surrender. However, certain types of term life insurance known as *deposit term* involve a cash value-like element that provides a partial endowment at the end of the term period and is generally payable only if the term insurance contract remains in force until the end of that period. It is possible that such a product or some variation of it could be included under the catch-all part of the covered product definition, and an insurer issuing only such a product might, therefore, become subject to the final rule concerning the establishment of an AML program.

Similarly, property and casualty products, title insurance, and health insurance policies have been excluded because their current features don't normally provide cash surrender values that might be used by money launderers. If an insurer was exempt from the final rule's AML requirements because of issuing only such insurance products, its offer of a property and casualty, title insurance, or health insurance product containing a cash surrender value could cause it to become subject to the AML program requirement.

Group life and annuity policies are considered products that pose low money-laundering risks. Since these policies are typically issued to a company or association, they normally restrict the control a covered participant has in manipulating or otherwise accessing contract values. Because of the low risk these policies involve, they are excluded from the definition of covered products.

Reinsurance and retrocession contracts are tools under which insurers reallocate the risks involved in their insurance activities between themselves. Since they involve negotiations between insurers rather than transactions with customers, they appear to involve little or no risk they will be used for money laundering.

1.18.3 Covered Products Must be Integral Part of Business

Not all issuers of covered insurance products are necessarily included under the final rule requiring the establishment of an AML program. The final rule adds an additional element to the definition of an insurance company subject to the rule: the person engaged in the issuing and underwriting of a covered product must be doing so *as a business*, rather than as an incidental part of a noninsurance business.

While this additional element is unlikely to affect many insurers, it clearly affects those tax-exempt organizations offering charitable gift annuities and similar insurance products as a vehicle for planned charitable giving to the tax-exempt organization offering them. The rationale for excluding these organizations from the AML requirement is the same as that applicable to insurers issuing only non-covered products. Specifically, they present a much lower risk of being used for money laundering or for the financing of terrorist agendas than those persons offering a covered product as an integral part of their business.

1.19 Summary

- Title III of the USA PATRIOT Act:
    - Broadens the definition of the term financial institution for purposes of anti-money laundering compliance;
    - Imposes significant due diligence and other requirements on financial institutions;
    - Increases the government's forfeiture powers and other sanctions for violations; and
    - Includes measures designed to improve information sharing and cooperation between financial institutions and law enforcement.

- Under the USA PATRIOT Act, "financial institution" is defined to include any business or agency that
    - employs more than 30 employees;
    - generates annual revenues in excess of $2 million;
    - maintains offices both within and outside the United States; and
    - engages in any activity that involves the exchange of funds.

- Life insurance companies are considered financial institutions under the USA PATRIOT Act and are required to implement AML programs for covered products.

1. When did Congress enact the Bank Secrecy Act?

   A. 1970 **Your answer is correct. Congress enacted the Bank Secrecy Act (BSA) in 1970. The purpose of the BSA is to prevent banks and other financial services institutions, including life insurance companies, from being used to hide the transfer or deposit of illegally obtained funds or from being used as intermediaries for this purpose.**
   B. 1980 **Your answer is incorrect. The BSA was not enacted in 1980.**
   C. 1960 **Your answer is incorrect. The BSA was not enacted in 1960.**
   D. 1950 **Your answer is incorrect. The BSA was not enacted in 1950.**

2. Which Treasury Department agency is charged with oversight and implementation of anti-money laundering laws?

   A. FINRA **Your answer is incorrect. FINRA is not charged with oversight and implementation of anti-money laundering laws.**
   B. FinCEN **Your answer is correct. FinCEN is an agency of the Treasury Department. It is charged with oversight and implementation of the federal anti-money laundering laws. It passes along intelligence to state, federal, and international law enforcement agencies and financial industry regulators to help them in their efforts to combat money laundering.**
   C. CIA **Your answer is incorrect. The CIA is not charged with oversight and implementation of anti-money laundering laws.**
   D. FBI **Your answer is incorrect. The FBI is not charged with oversight and implementation of anti-money laundering laws.**

3. Which Title of the USA PATRIOT Act is most relevant to financial institutions including life insurance companies?

   A. Title I **Your answer is incorrect. Title I is not most relevant to financial institutions.**
   B. Title II **Your answer is incorrect. Title II is not most relevant to financial institutions.**
   C. Title III **Your answer is correct. Title III of the Act, entitled the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, is most relevant to financial institutions including life insurance companies.**
   D. Title IV **Your answer is incorrect. Title IV is not most relevant to financial institutions.**

AML Program Compliance

One area of the USA PATRIOT Act that life insurers issuing covered products must be concerned with is the requirement to develop and implement an AML compliance program.

In this section you learn about the key provisions concerning development and implementation of an AML compliance program.

1.20 Overview

The USA PATRIOT Act requires life insurers issuing covered products to develop and implement an AML program that prevents the company from being used for money laundering. The plan must be in writing and approved by the insurer's senior management. In addition, the plan must generally meet the minimum legal requirements for AML plans for financial institutions.

The Treasury Department has conceded there is no "one size fits all" solution. Instead, the insurer’s AML plan must be based on an assessment of the money laundering risks associated with the insurer’s particular products, customers, distribution channels, and locations.

1.21 Minimum Requirements

Again, the USA PATRIOT Act does not specify the specific provisions that must be included in a company’s AML plan. Instead, the Act sets forth certain minimum requirements a plan must address. The way each requirement is addressed depends on the company’s particular situation.

The minimum requirements for a financial institution’s AML plan are as follows:

- Written internal policies, procedures, and controls;
- A designated compliance officer;
- An ongoing employee training program; and
- An independent auditing function to test the programs.

An insurer’s AML program must be:

- A written program;
- Approved by the insurer’s senior management; and

- Reasonably designed to prevent the insurer from being used to facilitate:
    - Money laundering, or
    - Financing terrorist activities.

The program must be made available to the Department of Treasury, FinCEN, or its designee upon request. While that template is broad, the final rule also offers guidance with respect to the AML program's minimum requirements.

Pursuant to the final rule, the insurer needs to consider all the relevant factors that affect the money-laundering and terrorist-financing risks to which it is exposed in the sale and marketing of its covered products. To illustrate such a risk-based approach, an insurer would be expected to consider:

- Its customers' use of cash or cash equivalents to pay premiums for covered products; and
- Whether the company underwrites and issues covered products to customers in any of the following jurisdictions:
    - Jurisdictions whose government has been identified by the State Department as a sponsor of international terrorism;
    - Jurisdictions designated by the FATF as non-cooperative with international AML principles; or
    - Jurisdictions determined by the Secretary of the Treasury or FinCEN as requiring special measures due to money laundering concerns.

Accordingly, an insurer issuing covered products must do all of the following in order to be in compliance with the final rule:

- It must take reasonable steps to identify the parts of its operations that may give rise to applicable Bank Secrecy Act requirements or that are vulnerable to money laundering or terrorist financing activity;
- Based on its identification of the BSA regulatory requirements and an assessment of its vulnerabilities with respect to money laundering and terrorist financing, it must develop and implement a program that is reasonably designed to:
    - Achieve regulatory compliance, and
    - Prevent money laundering or terrorist financing activity.
- Finally, it must monitor the effectiveness of its AML program.

An insurer's AML program must include—at a minimum—the following components. First, the insurance company issuing covered products must designate an AML compliance officer who will be responsible for the day-to-day operation of the AML program. The AML compliance officer may be a single person or a committee charged with the compliance responsibility. Further, the compliance officer position

may be full-time or part-time, depending on the insurer's assessment of the risks involved.

Irrespective of whether the compliance officer is a single person or a group of individuals in committee, the compliance officer must possess a significant level of knowledge consistent with the requirements of the task. That knowledge must include a thorough familiarity with all of the following:

- The insurer's business operations;
- All aspects of the insurer's AML program;
- The requirements of the Bank Secrecy Act; and
- Appropriate FinCEN forms.

Second, the insurer must develop AML policies, procedures, and internal controls based on its assessment of the money laundering risk associated with its business and which are designed to enable the insurer to:

- Comply with BSA requirements; and
- Prevent its being used by money launderers.

The insurer's assessment of its money laundering risk exposure should take into account the:

- Types of customers and locations it serves;
- Distribution channels employed; and
- Products it offers for sale.

Third, the insurer's AML program must provide for the initial and ongoing training of appropriate persons concerning their responsibilities under the program. This component must:

- Determine the type of training required, if any, to ensure employees are sufficiently trained to perform their duties under the AML program; and
- Direct the appropriate training to:
    - Employees,
    - Agents, and
    - Brokers.

Fourth, the insurer's program must include periodic testing by someone other than the compliance officer to determine if the AML program:

- Complies with the final rule, and
- Functions as designed.

Of course, these are only the minimum requirements and in order to have a successful AML plan; a company may choose to go well beyond the minimum.

1.22 Summary

- Financial institutions including insurers issuing covered products are required to implement and develop AML programs.
- The plans must be in writing approved by senior management.
- The plans must meet certain minimum requirements specified in the statute and final rule.

1. The USA PATRIOT Act provides a financial institution includes any business or agency that employs more than _____ employees, amongst other things.

A. 20 **Your answer is incorrect. The correct reply is not 20 employees.**
B. 10 **Your answer is incorrect. The correct reply is not 10 employees.**
C. 100 **Your answer is incorrect. The correct reply is not 100 employees.**
D. 30 **Your answer is correct. Under the USA PATRIOT Act, a "financial institution" is defined to include any business or agency that: Employs more than 30 employees; generates annual revenues in excess of $2 million; maintains offices both within and without the US; and engages in any activity that involves the exchange of funds.**

2. The term "financial institution" applies to which of the following?
   I. Life insurance companies
   II. Property-Casualty insurance companies
   III. Health insurance companies
   IV. Health insurance company agents

A. I only **Your answer is correct. The term "financial institution" has been interpreted to apply only to life insurers. Property-casualty and health insurance companies and their agents are not covered under the law.**
B. I and II **Your answer is only partially correct.**
C. II and III **Your answer is incorrect. "Financial institution" does not apply to property-casualty and health insurance companies.**
D. III and IV **Your answer is incorrect. "Financial institution" does not apply to health insurance companies and their agents.**

3. Which term refers to the fact that life insurance policies can be transferred and retransferred, making it difficult to determine the original source of funds?

A. Switching **Your answer is incorrect. Switching does not refer to the fact that life insurance policies can be transferred and retransferred, making it difficult to determine the original source of funds.**

B. Transferability **Your answer is correct. Transferability refers to the fact that life insurance policies and annuities can be transferred and retransferred by the owner to another individual or entity, making it difficult to determine the original source of the funds.**
C. Fixing **Your answer is incorrect. Fixing does not refer to the fact that life insurance policies can be transferred and retransferred, making it difficult to determine the original source of funds.**
D. Money laundering **Your answer is incorrect. Money laundering does not refer to the fact that life insurance policies can be transferred and retransferred, making it difficult to determine the original source of funds.**

CUSTOMER IDENTIFICATION PROGRAMS

The USA PATRIOT Act requires certain financial institutions to verify the identity of all customers, foreign and domestic. While life insurers issuing covered products are required to identify certain red flags that may indicate illegal activity—including a customer's reluctance to provide identifying information, or providing fictitious information, when purchasing a covered product—and file a suspicious activity report when appropriate, no specific reference to CIP programs for insurers is contained in the final rules.

In this section you learn about the key provisions concerning Customer Identification Programs (CIPs) applicable to certain financial institutions.

1.23 Overview

Section 326 of Title III requires financial institutions to create and implement what is referred to as a **customer identification program (CIP)**. The goal of such a program is to establish a process whereby institutions verify the identity of each customer or member at the time an account is opened.

After months of speculation and anticipation, the Treasury Department issued final regulations implementing the CIP requirements on April 30, 2003. Most financial institutions across the nation were required to comply with this regulation by October 1, 2003. Pursuant to the final rules concerning AML programs and SAR filings, life insurance companies are required to have procedures in place that are reasonably designed to obtain customer-related information from their insurance agents and brokers necessary to detect suspicious activity. The specific means of obtaining that customer-related information are left to the insurance companies' discretion. The final rules do not include any reference to customer identification programs for insurance companies—programs that are clearly required for broker-dealers and certain other financial institutions.

Although life insurers have discretion in the methods employed to obtain customer-related information for purposes of SAR filing, existing regulations applicable to bankers and broker-dealers may provide some guidance.

1.24 Minimum CIP Requirements for Certain Financial Institutions

To comply with the final regulations a financial institution must, at a minimum:

- Adopt a written CIP that is part of its AML program and that is appropriate to the financial institution's size and type of business;

- Verify the identity of any person seeking to open an account, to the extent reasonable and practicable;
- Maintain records of the information used to verify the person's identity; and
- Determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to brokers or dealers by any government agency.

1.25 Coverage

Very basically, the CIP must provide reasonable procedures for verifying the identity of **customers**, to the extent reasonable and practicable. In general, verification must occur within a reasonable time before or after the customer's **account** is opened or the customer is granted authority to effect transactions with respect to an account.

The final regulations define *customer* as "a person that opens a new account." This means the person identified as the account holder, including individuals, business entities, and representatives of minors or informal groups. The final regulations require the financial institution to know the identity of a trustee, but not beneficiaries of a trust.

The final rules exclude from the definition of "customer" certain readily identifiable entities, including:

- Financial institutions regulated by a federal functional regulator;
- Banks regulated by a state bank regulator; and
- Entities such as governmental agencies and instrumentalities and companies that are publicly traded.

In general, existing customers are also excluded from the definition of *customer*, provided the financial institution has a reasonable belief it knows the true identity of the person.

The term *account* is broadly-defined to cover banking relationships such as deposit accounts, transaction or asset accounts, extension of credit, safe deposit rental and cash management, custodian or trust services. Cash accounts, margin accounts, prime brokerage accounts and accounts established to engage in securities repurchase transactions are cited as examples of "accounts" in connection with securities brokerage.

Accounts acquired through acquisitions, mergers, or purchase and accounts opened for employee benefit plans are not considered "accounts" subject to the CIP.

Although life insurers issuing covered products are required to obtain customer-related information from their agents and brokers, no specific CIP requirement is imposed by the final rules. Guidance in gathering customer-related information, however, can be gleaned from the final regulations applicable to other financial institutions. For example, life insurance companies should be able to exclude certain existing customers, publicly-traded companies, minors, and trust beneficiaries from the requirement to obtain customer-related information. Furthermore, annuities and life insurance policies acquired through a merger or purchase may be excluded from the definition of accounts in the same way that brokerage and banking accounts acquired by merger or purchase are excluded.

1.26 Identification and Verification

In general, the final CIP regulations require procedures be established to take a **risk-based** approach to verifying the identity of customers. A risk-based approach means the procedures must be based on an assessment of the relevant risks, including the following:

- Those presented by the various types of accounts maintained by the financial institution;
- The various methods of opening accounts;
- The various types of identifying information available; and
- The financial institution’s size, location, and customer base.

At a minimum, a financial institution should obtain a customer’s:

- Name;
- Date of birth
- Address; and
- Identification number.

The customer’s identity must be verified within a reasonable time after the account is opened. Both documentary and nondocumentary means of verification such as automated identity verification are acceptable. Acceptable forms of legally valid **primary identification** include a:

- Driver's license with a photograph;
- U.S. Passport, or
- Alien registration card.

Acceptable forms of **secondary identification** may include the following:

- College photo identification;
- Major credit card that's active;
- Employer identification card; and

- Current utility bill from the customer's current residence.

In general, information relating to verification of a customer's identity must be retained for five years after the record of the information is made.

1.27 Procedures for Opening Personal Accounts

The legal requirements for a compliant CIP translate into specific procedures that should be observed in opening new customer accounts. In general, account representatives should determine if the customer's residence is nearby. If not, the account representative should obtain a reasonable explanation as to why the customer is opening the account at this office. It is also recommended that account representatives:

- Call the customer's place of residence or employment to confirm that the phone number is valid; and
- Obtain a prior bank or business reference.

Depending on the nature of or risk posed by the account, additional due diligence may be required of the account representative:

- Obtain information about the source of the customer's assets and income to determine whether the financial information is consistent with the customer's lifestyle;
- Obtain information on the customer's likely transaction patterns to identify unusual transactions or patterns that may occur;
- Require customers to have actual street addresses—P.O. Boxes or mail drop addresses are insufficient;
- Periodically contact the customers to update their information; and
- Conduct credit history and criminal background checks.

In general, account representatives should obtain all required documentation before or within a few days of opening a new account. In addition, the following precautions should be observed:

- Resist reliance on facsimile copies of documents during the account opening process.
- Make sure that all information is complete on the new account application.
- Be wary of customers who live outside your service area, particularly those who live outside the United States.
- Be wary of new account customers who want to use a post office box as an address.
- Be wary of customers that request the financial institution to hold all statements and correspondence.

Other precautions include:

- Be wary of customers who open multiple accounts in one or more names for no apparently legitimate reason.

- Be wary of a customer's reluctance or refusal to provide standard information and documentation during the account opening process. If a customer refuses to provide any of the information requested, do not open the account. If an existing customer fails to provide any requested information, consider ending the relationship with that customer; and
- Do not allow the sales goals to compromise due diligence efforts.

1.28 Procedures for Opening Business Accounts

In addition to verifying the identity of the person opening a new business account, you should also:

- Obtain evidence of legal status (is the business a corporation, partnership, sole proprietorship, or limited liability company);
- Consider checking the name of the business with a credit bureau or information reporting agency;
- Obtain and check prior bank or other references;
- Call the business to confirm whether the phone number is valid;
- Where practical, drive by the business to confirm whether it's operating at the address provided; and
- Obtain a financial statement.

Certain types of businesses, such as currency exchanges, wire transmitters, and import/export companies, present a higher risk of money laundering activity. Before opening such accounts you should:

- Obtain a description of the customer's principal line of business and primary trade area.
- Obtain a description of the customer's business operations, anticipated trading activity, total sales and anticipated international transactions.
- Obtain a list of major customers and suppliers.
- Obtain information on the company (if available) from a source such as a Dun & Bradstreet report or a credit report.

1.29 High-Risk Accounts

In connection with **high-risk accounts** it may be appropriate to use third-parties, such as credit bureaus, other financial institutions or other references, to authenticate the individual's identity and the source and legitimacy of funds. High risk accounts include, but are not limited to, the following:

- Private banking accounts;
- Trust accounts;
- Accounts held in other specialized departments;
- Accounts expected to have international transactions, especially to countries or jurisdictions considered to be secrecy or money laundering havens; and
- New accounts opened with large deposits, especially cash.

If an account is expected to have international transactions, especially to countries or jurisdictions considered to be secrecy or money laundering havens, account representatives should take appropriate actions to determine the identities of the true owners of the account. They should also take reasonable actions to identify the source of the funds being deposited.

Large deposits at account opening, especially cash, should be questioned, and reviewed for their legitimacy. Again, reasonable actions should be taken to evaluate the source of the funds.

1.30 Comparison with Government Lists

The financial institution's CIP must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. Checking the OFAC "Specially Designated Nationals and Blocked Persons List" or "SDN" must be done within a reasonable time after the account is opened or earlier if required by federal law, regulation or directive.

1.31 Customer Notice

The law requires "adequate notice" be provided to customers before the financial institution requests any identification information. The notice may be given in any manner reasonably designed to ensure the customer is able to view or get the notice before opening the account, such as by lobby poster, website, or on account applications.

1.32 Summary

Section 326 of Title III requires certain financial institutions to create and implement what is referred to as a *customer identification program* (CIP).

- At a minimum, financial institutions must adopt and implement a written CIP that provides for:
    - Verifying the identity of any person seeking to open an account, to the extent reasonable and practicable;
    - Maintaining records of the information used to verify the person's identity; and
    - Determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to brokers or dealers by any government agency.
- Customers must receive adequate notice before the financial institution requests identification information.

1. Written internal policies, procedures, and controls; a designated compliance officer; an ongoing employee training program; and an independent audit function to test the programs are minimum requirements for a financial institution's _____ plan.

A. BSA **Your answer is incorrect. This is not a requirement of the financial institution's BSA plan.**
B. MLCA **Your answer is incorrect. This is not a requirement of the financial institution's MLCA plan.**
C. AML **Your answer is correct. The minimum requirements for a financial institution's AML plan are as follows: Written internal policies, procedures, and controls; A designated compliance officer; An ongoing employee training program; and An independent audit function to test the programs.**
D. Oversight **Your answer is incorrect. This is not a requirement of the financial institution's Oversight plan.**

2. The Treasury Department directs that an insurer's AML must be based on assessment of risk of which of the following?

I. Products
II. Customers
III. Distribution Channels
IV. Location

A. II only **Your answer is only partially correct.**
B. II and III **Your answer is only partially correct.**
C. III and IV **Your answer is only partially correct.**
D. I, II, III and IV **Your answer is correct. The Treasury Department has conceded that there is no "one size fits all" solution. Instead, the insurer's AML plan must be based on an assessment of the money laundering risks associated with the insurer's particular products, customers, distribution channels, and locations.**

3. The program created to verify the identity of each customer or member at the time an account is opened is called what?

A. CIP **Your answer is correct. Section 326 of Title III requires financial institutions to create and implement what is referred to as a customer identification program (CIP). The goal of such a program is to establish a process whereby institutions verify the identity of each customer or member at the time an account is opened.**
B. AML **Your answer is incorrect. The program is not called the AML.**

C. VIP **Your answer is incorrect. The program is not called the VIP.**
D. LIP **Your answer is incorrect. The program is not called the LIP.**

SUSPICIOUS ACTIVITY REPORTS

Another area of the USA PATRIOT Act life insurers must be concerned with is the requirement for filing Suspicious Activity Reports (SARs).

In this section you learn about the key provisions concerning Suspicious Activity Reports. After completing this section, you will be able to:

- *Define a SAR;*
- *Explain the circumstances under which a SAR must be filed;*
- *Identify red flags for SARs;*
- *Identify the time frame for filing a SAR;*
- *Identify the documentation that must accompany a SAR;*
- *Discuss the prohibition against customer notification; and*
- *Explain the significance of the safe-harbor protection associated with SARs.*

1.33 Overview

On July 1, 2002, the Treasury issued final regulations requiring all broker-dealers to file SARs in certain circumstances.

Basically, SARs must be filed whenever customers engage in suspicious or unusual activities that might suggest they are involved in money laundering. This suggests that customer activity should be monitored on an ongoing basis. The purpose for filing a SAR is to alert regulators and FinCEN to possible criminal actions, including money laundering.

Insurance agents and brokers and home office underwriters and policy owner service personnel are probably in the best position to monitor customer activity. Although insurers are not subject to the CIP requirements applicable to other financial institutions, they are required to file SARs when they believe a customer may be involved in illicit activity; a red flag indicating possible illicit activity is a customer's reluctance to provide identifying information, or providing fictitious information, when purchasing an insurance product.

A starting place for monitoring customer activity is for the agent or broker to obtain a complete **customer profile** identifying customer characteristics, needs, objectives, and typical financial transactions. The customer profile can be used to establish a baseline about typical customer behavior and also serves as a benchmark against which suspicious activity can be spotted.

Customer accounts should be monitored on an ongoing basis to identify unusual transactions, based on the customer's profile. Financial institutions should be on the alert for transactions:

- Outside the customer's normal transaction pattern; and

- Abnormal for the business.

Account representatives should ask, based on their knowledge of the customer, if the transaction seems out of the ordinary. If the answer is *yes*, at a minimum further investigation and review is appropriate. Filing of a SAR may also be appropriate.

1.34 Activities Requiring the Filing of a SAR

The law and regulations identify certain activities that are so troubling they require filing a SAR. A financial institution must file a SAR whenever it becomes aware of the following types of activities:

- Insider abuse at the financial institution involving any amount;
- A violation of a federal law that aggregates to $5000 or more, provided a suspect can be identified;
- A violation of federal law that aggregates to $25,000 or more, regardless of whether a suspect can be identified;
- Transactions that aggregate to $5000 or more that involve potential money laundering or violations of the BSA; and
- Intrusion into the financial institution's computer system to steal or change account or customer information or affect critical computer systems.

Other activities that clearly merit filing of a SAR include:

- A new individual customer or business asks for exemption from Currency Transaction Report filings;
- A customer appears to withhold part of a currency deposit or withdrawal in order to fall below the $10,000 filing threshold for a Currency Transaction Report;
- A customer is reluctant to provide information necessary for filing a mandatory report or to complete identification or authentication information requested by the financial institution;
- A customer tries to force or bribe a financial institution employee into not filing any required record keeping or reporting forms;
- A customer uses an ATM to make several cash deposits that are just below a reporting threshold; and
- A customer has unusually large deposits of U.S. food stamps (which are sometimes exchanged for narcotics).

In addition to these activities that mandate the filing of a SAR, certain other activities are likely to require the filing of a SAR.

1.35 Red Flags for a SAR

Certain customer activities, while not requiring the filing of a SAR, should raise suspicions. These activities are referred to as ***red flags*****.**

In general, employees of financial institutions should consider filing a SAR if:

- A customer makes frequent large dollar deposits or withdrawals with no explanation as to how they will be used and/or the customer's business is not the type that would usually deal in such large amounts;
- A domestic business account that would not normally be expected to have international funds transfers begins to make frequent transfers to offshore accounts;
- A customer has a number of accounts and frequently transfers funds between the accounts for no apparent legitimate reason;
- A large quantity of cashier's checks, money orders, and/or wire transfers are deposited into an account, inconsistent with the profile of the account holder; and
- An account history shows little or no regular activity, and the account appears to be used primarily as a short-term repository for funds that are then transferred outside the U.S. (especially to tax haven countries); and
- A customer makes numerous cash deposits, quickly followed by lump-sum funds transfers to offshore accounts.

Activities that constitute red flags vary from industry to industry. The following are examples of red flags for life insurance:

- The customer's lack of concern with the cost of the policy;
- Large single payments for life insurance or annuities;
- Beneficiaries are unidentified or are located in countries known for illegal activities;
- Premiums and/or face amounts are inconsistent with customer's income and/or net worth;
- Premium payments are made by apparently unrelated parties;
- The policy is assigned to a third-party soon after it is purchased; and
- Early policy cancellation.

Keep in mind these are examples only and not an exhaustive list. Also, it is important to keep in mind that customers are not engaged in illegal activities merely because their activities mirror one or more of these activities. However, such behavior warrants further review and/or investigation.

1.36 Time for Filing a SAR

A financial institution must file a SAR within 30 calendar days after detecting the facts that formed the basis for filing the SAR.

If the institution is unable to identify a suspect on the date of initial detection, the SAR filing may be delayed for an additional 30 calendar days. This extension allows the financial institution to conduct an investigation to try to identify the suspect.

In any event, the SAR must be filed within 60 calendar days after the date when the reportable transaction was initially detected, even if the institution hasn't completed the investigation.

In either case, the time frame for filing a SAR begins from the first time the financial institution has any facts indicating illegal or suspicious activity has occurred.

Once a financial institution files a SAR, a copy of the SAR and all supporting documents must be retained for five years from the date the SAR was filed.

1.37 SAR Filing Required of Insurance Agents or Brokers

The requirement for insurance companies to file a SAR began in 2005. Insurance companies are required to create an anti-money laundering program *and* submit appropriate SARs as mandated by FinCEN. The SARs should be filed to report suspicious activities applicable to insurance companies issuing covered products. The FinCEN specifies their rule applies to insurance companies issuing or underwriting certain products that present a high degree of risk for money laundering, terrorist financing or illicit activities. The insurance products specifically subjected to the rule on insurance AML programs and SAR filings include:

- *Permanent life insurance policies, other than group life insurance policies*
- *Annuity contracts, other than group annuity contracts*
- *Any other insurance products with features of cash value or investment features*

At minimum, insurance companies subject to the rule requiring an anti-money laundering program must establish a program that comprises ***four basic elements****:*

1. *A compliance officer who is responsible for ensuring that the program is implemented effectively*
2. *Written policies, procedures, and internal controls reasonably designed to control the risks of money laundering, terrorist financing, and other financial crime associated with its business*
3. *Ongoing training of appropriate persons concerning their responsibilities under the program*
4. *Independent testing to monitor and maintain an adequate program*[1]

[1] FinCen Press Release: *Insurance Companies Required to Establish Anti-Money Laundering Programs and File Suspicious Activity Reports*

1.38 Supporting Documentation

When filing a SAR, there is no need to file supporting documentation unless specifically requested during the filing process. The financial institution must, however, provide such documentation to the appropriate law enforcement and regulatory authorities upon request. These authorities are not required to provide a subpoena or other court order.

Insurance companies or financial institutions and their agents and employees should avoid providing too much information to law enforcement and regulatory authorities. Customer information that goes beyond that necessary to support the SAR should remain private unless such information is specifically requested in a subpoena or it is determined there is another legal basis for voluntarily sharing such information.

1.39 Prohibition Against Customer Notification

In an effort to provide legal and regulatory authorities with an edge against suspected money launderers, financial institutions and their employees and agents that file SARs are prohibited from notifying the customer (or any other person involved in the transaction) that a report has been filed. If customers were alerted to the filing of a SAR, money launderers could take advantage of the opportunity to cover their tracks or leave the country.

Any financial institution that receives a request for information related to a SAR from:

- The subject of the SAR
- One of his or her agents
- Someone who might report the SAR filing back to the party on whom the SAR was filed (such as an attorney for the party)

should not confirm it filed a SAR. Instead, the financial institution should merely state it complies with its legal requirements. It should then immediately notify its regulator and FinCEN that such a request was made.

This prohibition on notification includes responses to legal documents, such as a request for documents or other information made during the course of a lawsuit.

1.40 SAR Safe Harbor

A concern associated with the filing of SARs is the customer/subject of the SAR could sue and hold the financial institution (and employees and agents) liable for breach of privacy. This concern is legitimate, because most states and the federal courts recognize a cause of action for revealing a customer's private information. Even if the customer's lawsuit was successfully defended, there could be significant cost in attorney's fees and lost time.

Congress has addressed this concern by providing a broad **safe harbor** from civil liability to financial institutions and employees that file SARs. In general, safe harbor is a set of circumstances, described in the statute, under which a customer's lawsuit will not be rewarded.

Federal law provides safe harbor protection from civil liability for all reports of suspected or known criminal violations and suspicious activities to appropriate authorities, including supporting documentation, even when the reports are filed on a voluntary basis. Note the safe harbor is available only when the customer information is provided to appropriate authorities. In general, customer privacy must be respected.

While there is a safe harbor for filing a SAR, there is no protection against "looking the other way." In fact, the law has a name for ignoring suspicious money laundering activity. The term given to this is **willful blindness.** Basically, if the customer activity was such that the financial institution or its employees were aware or should have been aware of suspicious activity, appropriate action including filing a SAR is required. Failure to take appropriate action in such situations can lead to prosecution and sanctions.

1.41 Employee Activities Meriting the Filing of a SAR

The foregoing discussion focused on filing SARs in connection with customer activities. However, suspicious activities by employees may also require the filing of SARs.

For example, the following activities merit the filing of a SAR:

- An employee shows reluctance or refuses to conform to the institution's policies and procedures, claiming that they don't work for his customers;
- An employee lives a lifestyle that appears to be well beyond his or her means;
- An employee is reluctant to take a long vacation;
- An employee advises a customer on how to avoid a reporting requirement; and
- An employee fails to perform any due diligence on a customer, especially an international customer who performs large transactions

Being watchful and alert in the workplace is not just a good practice; it is the law.

1.42 BSA eFiling System

Suspicious Activity Reports filed by insurance companies must be done using the BSA eFiling System. There is a single SAR form on which you indicate the industry from which you are reporting. As such, *technically,* there is no longer a Form 101, but rather, you create an account on the BSA eFiling system and report your suspicious activities online. Cash Transaction Reports (CTRs f/k/a form 108 or 8300) are also filed using the BSA eFiling System.

1.43 Summary

- SARs must be filed whenever customers engage in suspicious or unusual activities that might suggest they are involved in money laundering.
- A SAR must generally be filed within 30 calendar days after detecting the facts that formed the basis for filing the SAR.
- When filing a SAR, there is no need to file supporting documentation.

- Companies, their employees, and agents that file SARs are prohibited from notifying the customer, any agent/affiliate of the customer, or any other person involved in the transaction, that a report has been filed.
- Federal law provides safe harbor protection from civil liability for all reports of suspected or known criminal violations and suspicious activities to appropriate authorities, including supporting documentation.
- While there is a safe harbor for filing a SAR, there is no protection against willful blindness in ignoring a suspicious activity.
- Employee activity may also be the subject of a SAR.

1. CIP Regulations require a financial institution know the identities of the following account holders:
   - I. Individuals
   - II. Trustees
   - III. Business Entities
   - IV. Beneficiaries of a Trust

   A. I only **Your answer is only partially correct.**
   B. I, II and III **Your answer is correct**. **The final regulations define "customer" as "a person that opens a new account." This means the person identified as the account holder, including individuals, business entities, and representatives of minors or informal groups. The final regulations require the financial institution to know the identity of a trustee, but not beneficiaries of a trust.**
   C. II and III **Your answer is only partially correct.**
   D. III and IV **Your answer is only partially correct.**

2. Which of the following are defined as accounts that cover banking relationships under the CIP?
   - I. Asset Accounts
   - II. Deposit Accounts
   - III. Accounts acquired through merger
   - IV. Employee benefit plans

   A. III and IV **Your answer is incorrect. Accounts acquired through merger and employee benefit plans are not accounts that cover banking relationships under the CIP.**
   B. I and IV **Your answer is only partially correct.**
   C. I and II **Your answer is correct. The term "account" is broadly defined to cover banking relationships such as deposit accounts, transaction or asset accounts, extensions of credit, safe deposit rentals and cash management, and custodian or trust services. Cash accounts, margin accounts, prime brokerage accounts and accounts established to engage in securities repurchase transactions are cited as examples of**

"accounts" in connection with securities brokerage. Accounts acquired through acquisitions, mergers, or purchase and accounts opened for employee benefit plans are not considered "accounts" subject to the CIP.

D. I and III **Your answer is only partially correct.**

3. Private banking accounts, trust accounts and new accounts opened with large deposits would be considered what type of account?

A. Suspicious **Your answer is incorrect. While this could appear suspicious, it is not the optimal reply.**
B. New **Your answer is incorrect. While this is, in fact, a new account, it is not the optimal reply.**
C. Illegal **Your answer is incorrect. While this could appear illegal, it is not the optimal reply.**
D. High Risk **Your answer is correct. High risk accounts include, but are not limited to, the following:**

- **Private banking accounts;**
- **Trust accounts;**
- **Accounts held in other specialized departments;**
- **Accounts expected to have international transactions, especially to countries or jurisdictions considered to be secrecy or money laundering havens; and**
- **New accounts opened with large deposits, especially cash.**

AML REGULATORS

Anti-money laundering laws are subject to regulation by a variety of agencies. These agencies and their functions are discussed in this section.

In this section you learn about the various state and federal agencies and authorities that regulate the AML activities of financial institutions. After completing this section, you will be able to:

- *Describe the role of FinCEN in AML regulation;*
- *Describe the role of the Office of Foreign Assets Control (OFAC).*

1.44 Overview

The Treasury Department has primary responsibility for enforcement of the BSA and the USA PATRIOT Act. However, compliance with these and other AML laws is monitored by a number of state and federal agencies.

Financial institutions, in general, are regulated by one of the following agencies:

- FinCEN;
- OFAC;
- The Comptroller of the Currency (OCC);
- The Federal Deposit Insurance Corporation (FDIC);
- State Banking Departments;
- State Insurance Departments;
- National Credit Union Association; and
- The Securities and Exchange Commission (SEC)

1.45 FinCEN

The primary BSA and anti-money laundering regulatory agency is the Financial Crimes Enforcement Network (FinCEN). FinCEN supports law enforcement agencies and fosters interagency and global cooperation to combat money laundering crimes. FinCEN is also an enforcement agency and can impose fines and refer matters for further action and prosecution.

FinCEN works closely with all of the financial regulatory agencies to enact rules and legislation for detecting and deterring money laundering.

1.46 OFAC

The Office of Foreign Assets Control (OFAC) is a division of the U.S. Department of the Treasury. It administers and enforces economic and trade sanctions against targeted foreign countries, organizations that sponsor terrorism, and international narcotics traffickers. These sanctions are based on U.S. foreign policy and national security goals.

OFAC acts under the Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of these sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

All U.S. businesses and all U.S. citizens and residents must comply with OFAC regulations. Most of the individuals, entities, businesses, groups, and government officials who are the subjects of these economic sanctions are identified by OFAC on its **Specially Designated Nationals (SDN) List**. Engaging in any financial transaction for a party who is on the SDN List may constitute money laundering.

1.47 OFAC Sanctions

In general, OFAC has the authority to administer the following sanctions on individuals and entities that fail to comply with applicable laws:

- Prohibit providing any goods or services to SDNs and others;
- Require blocking accounts and other assets belonging to the SDNs as well as other parties or entities subject to OFAC economic sanctions; and
- Require that blocked transactions be reported to OFAC within ten days.

Complying with these sanctions is an essential part of a financial institution's AML policies and procedures.

1.48 OFAC Compliance

Similar to the requirements under the BSA and USA PATRIOT Act, financial institutions are required to have an OFAC compliance program. Such a program should include written policies and procedures for screening transactions for possible OFAC violations.

As with a BSA compliance program, a financial institution must:

- Name a designated person responsible for OFAC compliance;
- Implement appropriate training and communication regarding OFAC's regulations;
- Conduct annual audits on OFAC compliance.
-

In addition, a financial institution's OFAC compliance program must include:

- Procedures for maintaining current lists of blocked countries, entities, groups, and individuals must be in place.
- Procedures for listing information must be provided to all employees who "need to know" such information to ensure compliance.
- Procedures for comparing all new accounts, with OFAC's SDN lists prior to being opened.

1.49 Summary

- The primary BSA and anti-money laundering regulatory agency is the Financial Crimes Enforcement Network (FinCEN).
- FinCEN supports law enforcement agencies and fosters interagency and global cooperation to combat money laundering crimes. FinCEN is also an enforcement agency and can impose fines and refer matters for further action and prosecution.
- OFAC administers and enforces economic and trade sanctions against targeted foreign countries, organizations that sponsor terrorism, and international narcotics traffickers.
- OFAC may impose a number of sanctions on financial institutions for failing to comply with applicable laws and regulations.
- Similar to the requirements under the BSA and USA PATRIOT Act, financial institutions are required to have an OFAC compliance program.

1. Whenever a customer engages in suspicious or unusual activities an agent or broker should file what?

A. A SAR **Your answer is correct. SARs must be filed whenever customers engage in suspicious or unusual activities that might suggest they are involved in money laundering. This suggests that customer activity should be monitored on an ongoing basis. The purpose for filing a SAR is to alert regulators and FinCEN to possible criminal actions, including money laundering.**
B. An AML **Your answer is incorrect. An AML is not the document that gets filed.**
C. A BAR **Your answer is incorrect. A BAR is not the document that gets filed.**
D. An MLR **Your answer is incorrect. An MLR is not the document that gets filed.**

2. A Suspicious Activity Report must be filed within how many days after the activity occurs?

A. 10 **Your answer is incorrect. A SAR does need to be filed but not within 10 days of the activity.**
B. 30 **Your answer is correct. A financial institution must file a SAR within 30 calendar days after detecting the facts that formed the basis of suspicion.**
C. 45 **Your answer is incorrect. A SAR does need to be filed but not within 45 days of the activity.**
D. 60 **Your answer is incorrect. A SAR does need to be filed but not within 60 days of the activity.**

3. Which agency has primary responsibility for enforcement of the USA PATRIOT Act?

A. FBI **Your answer is incorrect. The FBI is not the agency with primary responsibility for enforcement of the USA PATRIOT Act.**
B. CIA **Your answer is incorrect. The CIA is not the agency with primary responsibility for enforcement of the USA PATRIOT Act.**
C. Treasury Department **Your answer is correct. The Treasury Department has primary responsibility for enforcement of the BSA and the USA PATRIOT Act. However, compliance with these and other AML laws is monitored by a number of state and federal agencies.**
D. Congress **Your answer is incorrect. Congress is not the agency with primary responsibility for enforcement of the USA PATRIOT Act.**

Civil and Criminal Penalties and Sanctions for Non-Compliance

There are a number of civil penalties and criminal sanctions that financial institutions and employees can be subjected to, if they fail to comply with AML laws and regulations.

In this section you learn about the penalties and sanctions that apply to money laundering and noncompliance with applicable laws and regulations. After completing this section, you will be able to:

- *Describe the penalties and sanctions applicable to financial institutions;*
- *Describe the penalties and sanctions applicable to employees, officers, and directors of financial institutions.*

1.50 Federal Penalties Imposed on Financial Institutions for Money Laundering and Noncompliance

Financial institutions guilty of money laundering, or of failing to develop and implement adequate BSA policies and procedures are subject to a variety of civil and criminal penalties. The penalties can be imposed on the financial institution, its employees, officers, and directors.

Federal penalties for engaging in transactions involving money laundering, assisting with money laundering, or structuring a transaction to avoid a BSA or other reporting requirement include the following:

- Fines of not less than two times the amount of the laundered transactions;
- A civil penalty in an amount of not less than two times the amount of the transaction, but not more than $1 million on any financial institution that violates the correspondent account and private banking due diligence and reporting provisions of the USA PATRIOT Act;
- Fines of up to $500,000 for failing to meet basic BSA record keeping, reporting, and other anti-money laundering requirements; and
- A criminal penalty in an amount of not less than two times the amount of the transaction, but not more than $1 million on any financial institution that violates the correspondent account and private banking due diligence and reporting provisions of the USA PATRIOT Act.

These fines and penalties are assessed on a "per violation" basis, making it very expensive to avoid compliance or engage in money laundering activities.

In addition to the criminal fines and penalties discussed above, other penalties include the following:

- Civil fines for violating other laws and regulations (such as the obligation to operate in a safe and sound manner);
- Forfeiture of assets (including, but not limited to, loan collateral, entire bank accounts, interbank, and correspondent bank accounts, etc.);
- Revocation of the financial institution's charter.

1.51 Federal Penalties Imposed on Employees, Officers, and Directors for Money Laundering and Non-Compliance

Parallel fines penalties and sanctions can be applied personally to officers, directors, and employees of financial institutions. The federal penalties for engaging in transactions involving money laundering, assisting with money laundering, or structuring a transaction to avoid a BSA or other reporting requirement include the following:

- 20 years imprisonment;
- Fines of up to two times the amount of the laundered transactions or $500,000, whichever is greater; and
- Additional civil fines for violating other laws and regulations.

Again, similar to the penalties, fines, and sanctions imposed in financial institutions, these penalties are imposed on a per violation basis, making it extremely costly to engage in money laundering.

In addition, fines of up to $500,000 and five years imprisonment can result from the following types of crimes:

- Failing to file a report required by the BSA; or
- Filing a false or fraudulent report required by the BSA.

The bottom line is money laundering can lead to penalties severe enough to ruin a financial institution and the careers and lives of the employees, directors, and officers who work there.

1.52 Summary

- Both criminal guilt and civil liability can result from involvement in money laundering activities or BSA non-compliance.
- Penalties, sanctions, and fines may be assessed against the financial institution and employees, officers, and directors.

1. Who administers and enforces economic and trade sanctions against targeted foreign countries?

A. BSA **Your answer is incorrect. The BSA is not the administrator and enforcer of economic and trade sanctions against targeted foreign countries.**
B. CIP **Your answer is incorrect. The CIP is not the administrator and enforcer of economic and trade sanctions against targeted foreign countries.**
C. DOT **Your answer is incorrect. The DOT is not the administrator and enforcer of economic and trade sanctions against targeted foreign countries.**
D. OFAC **Your answer is correct. The Office of Foreign Assets Control (OFAC) is a division of the U.S. Department of the Treasury. It administers and enforces economic and trade sanctions against targeted foreign countries, organizations that sponsor terrorism, and international narcotics traffickers.**

2. Engaging in a financial transaction for or with a party on the OFAC's _____ list may constitute money laundering.

A. Specially Designated Nationals **Your answer is correct. ALL U.S. businesses and all U.S. citizens and residents must comply with OFAC regulations. Most of the individuals, entities, businesses, groups, and government officials who are the subjects of these economic sanctions are identified by OFAC on its Specially Designated Nationals (SDN) List. Engaging in any financial transaction for a party who is on the SDN List may constitute money laundering.**
B. Active Terrorists **Your answer is incorrect. It is not the Active Terrorists List.**
C. Foreign Nationals **Your answer is incorrect. It is not the Foreign Nationals List.**
D. Anti-Terrorism **Your answer is incorrect. It is not the Anti-Terrorism List.**

3. Engaging in money laundering, assisting with money laundering, or avoiding BSA reporting requirements subjects a financial institution to a fine of not less than _____ times the amount of the laundered transaction.

A. 5 **Your answer is incorrect. The fine is not five times the amount of the laundered transaction.**
B. 2 **Your answer is correct. Federal penalties for engaging in transactions involving money laundering, assisting with money laundering, or structuring a transaction to avoid a BSA or other reporting requirement include the following: Fines of not less than two times the amount of the laundered transactions; a civil penalty in an amount of not less than two times the amount of the**

transaction, but not more than $1 million on any financial institution that violates the correspondent account and private banking due diligence and reporting provisions of the USA PATRIOT Act; fines of up to $500,000 for failing to meet basic BSA record keeping, reporting, and other anti-money laundering requirements; and a criminal penalty in an amount of not less than two times the amount of the transaction, but not more than $1 million on any financial institution that violates the correspondent account and private banking due diligence and reporting provisions of the USA PATRIOT Act.

C. 10 **Your answer is incorrect. The fine is not ten times the amount of the laundered transaction.**

D. 3 **Your answer is incorrect. The fine is not three times the amount of the laundered transaction.**

AML Case Study: Insurance Agent

Case Study

John Thompson is a life insurance agent for MegaMutual who recently met with Paul Smith, a boyhood friend he hadn't seen in several years. When Paul learned John had become an insurance agent, he suggested they meet to talk about the purchase of a life insurance policy. Delighted with his good fortune, John met with Paul a few days later.

The Data-Gathering Interview

At the meeting Paul explained to John that he had become a real-estate agent working in the Miami, Florida area. Paul indicated that he was new to the real estate business but that he thought that his prospects were good. Now he thought it was the time to start building an estate. He indicated to John that insurance appealed to him because of the protections and guarantees life insurance policies provide.

John gathered the necessary data about Paul Smith and promised to return the following week with suggestions. The information John Thompson gathered on Paul Smith is summarized below:

Data-Gathering Form

Client: Paul Smith		**Age: 42** **Spouse's age: unmarried**
Dependent children	**None**	**Age:**
		Age:
		Age:
Annual earnings:	**Client: $32,500**	**Spouse**
Occupation	**Real estate agent**	**Spouse**

If retired, total annual family income:

Assets

Liquid:	**Non-liquid:**
Savings: $5000	**Personal property: $10,000**
Retirement Accounts: none	**Residence: $ 250,000**
Securities: $10,000	**Business interests: $500,000**
Other: none	**Vacation/rental property: none**
Monthly obligations	
Mortgage/ rent:	
Savings: $5000	
Food: $300	
Installment debt/ credit cards: none	
Utilities: $175	
Entertainment: $150	
Travel: $100	
Insurance: none	
Other: real estate taxes $450	

Objectives: begin retirement/ estate
Risk tolerance: moderate
Other:

Upon reviewing Paul's profile, John realized Paul appeared to have little or no need for life insurance. Nor did a deferred annuity seem suitable because of Paul's age, lack of liquidity, and modest income. However, Paul appeared to need disability income coverage that would pay him an income in the event he was injured and unable to work.

The Recommendation and Sale

John recommended a disability policy to Paul, but Paul said he didn't want to discuss that kind of policy and he had decided to buy a life insurance policy. Paul stated he wanted to purchase a $1 million universal life insurance policy. As an insurance agent, John was surprised but pleased with the possibility of such a substantial sale. He was even more surprised when Paul presented $9900 in cash to pay the first premium, explaining to John he didn't have a checking account and preferred to pay in cash. John was suspicious because he wondered how Paul could pay his other expenses in cash, particularly the $450 per-month real estate taxes on his residence. Paul told John it was none of his business and his (Paul's) only concern was whether he could withdraw the premiums in the event he needed the money.

Submitting the Application to the Insurer

John met with his agency manager, Peter Riccio, to discuss Paul's application for the $1 million life insurance policy. Peter definitely wanted to close the sale in order to keep his agency in good standing. He looked at the application and realized they needed to "package" the sale before sending it to the home office. Peter then told John to deposit the cash in his personal checking account and write a check to the company for the premium. He explained that MegaMutual would then be relieved of the burden of completing a Currency Transaction Report the insurance companies have to make on cash transactions of $10,000 or more.

He suggested to John that the purchase of a $1 million life insurance policy by a young unmarried individual with no children was somewhat unusual. Riccio told John in order to make it easier for the home office underwriter to issue the policy, John should alter the application by stating Paul was engaged to be married within the year. John complied, and the application along with the $9900 check was sent to MegaMutual for underwriting.

Review

Does John need to file a suspicious activity report?

Yes

Your answer is correct. Insurance brokers and agents are required to file SARs. The customer is attempting a suspicious transaction.

No

Your answer is incorrect. Insurance brokers and agents are required to file SARs. The customer is attempting a suspicious transaction.

What is John's obligation concerning any disclosure to MegaMutual?
John made a big mistake in following his manager's direction and misleading MegaMutual about the applicant's intention to marry in the near future. By doing that, he helped to disguise the inappropriateness of a young, unmarried individual's purchase of a large life insurance policy.

John is an agent and as such, is supposed to file a SAR. John has an obligation to provide relevant information concerning the applicant to MegaMutual, too. He should have disclosed to the insurer that a) the purchase of a $1 million life insurance policy was suggested by the applicant; b) it appeared excessive and unsuitable in light of Paul Smith's low level of liquidity and unmarried status; c) the applicant expressed concern about his ability to access cash value; and d) the applicant paid the initial premium in cash in an amount just below the CTR filing threshold.

Review
Were John's and his manager's actions appropriate?
Yes
Your answer is incorrect. Rather than acting as MegaMutual's "eyes and ears" concerning the applicant, they tried to obscure the unsuitability of the large life insurance purchase by suggesting it was made with the intention of providing income for a soon-to-be spouse. Further, depositing cash in the agent's account amounts to impermissible commingling and was clearly designed to obscure the currency transaction. This is a gigantic AML red flag.

No
Your answer is correct. Rather than acting as MegaMutual's "eyes and ears" concerning the applicant, they tried to obscure the unsuitability of the large life insurance purchase by suggesting it was made with the intention of providing income for a soon-to-be spouse. Further, depositing cash in the agent's account amounts to impermissible commingling and was clearly designed to obscure the currency transaction. This is a gigantic AML red flag.

Home Office Underwriting
When the application was received in MegaMutual's home off ice, Steve, the underwriter, noted that a $1 million life insurance policy for an unmarried person such as Paul Smith seemed excessive. However, after reading the Agent's Report that stated the insured planned to marry in the near future, he felt more comfortable with the amount. Since the amount was just below the amount at which an inspection report was required, no report was ordered. When the physical exam was received Steve approved the policy and sent it to Riccio's agency.

Review

Did MegaMutual and the home office underwriter handle Paul Smith's application appropriately?
Yes
Your answer is incorrect. Without additional information concerning the intended use of the $1 million life insurance policy, its purchase would appear clearly unsuitable - unless the undisclosed intention was to launder the premium. Appropriate disclosure on the Agent's Report - a disclosure that indicated the sale was initiated by the applicant who expressed concern only about his ability to withdraw the funds and paid premiums in cash - is a red flag requiring the filing of a SAR. The underwriter should, nonetheless, have inquired about the reason for the application. At the very least, the application should have been reduced in size and/or suspended until the applicant married. In addition, the payment of an initial premium that exceeds 30% of the applicant's gross income is suspicious, considering the absence of significant assets, and suggests the money came from an undisclosed source-another AML red flag.

No
Your answer is correct. Without additional information concerning the intended use of the $1 million life insurance policy, its purchase would appear clearly unsuitable - unless the undisclosed intention was to launder the premium. Appropriate disclosure on the Agent's Report - a disclosure that indicated the sale was initiated by the applicant who expressed concern only about his ability to withdraw the funds and paid premiums in cash - is a red flag requiring the filing of a SAR. The underwriter should, nonetheless, have inquired about the reason for the application. At the very least, the application should have been reduced in size and/or suspended until the applicant married. In addition, the payment of an initial premium that exceeds 30% of the applicant's gross income is suspicious, considering the absence of significant assets, and suggests the money came from an undisclosed source-another AML red flag.

Delivering Smith's New Policy
Smith's policy was received in the agency two days later, and John made an appointment to deliver it to his new client. During the delivery interview John discussed Paul's new policy with him. Paul did not seem interested in the details but only wanted again to be assured he could withdraw the cash value if and when he needed it. John assured him he could. Paul gave John an additional cash premium payment of $9900.

The Withdrawal
Three months after buying the life insurance policy Smith contacted MegaMutual and requested the maximum withdrawal of funds. He directed that the $17,500 withdrawal check—the net amount after payment of $2000 in surrender charges—be sent to his brother in Belarus. Paul Smith made no further premium payments and the policy lapsed shortly afterward.

Review: The Withdrawal

Regarding Smith's withdrawal transaction, which of the following are red flags that require MegaMutual to file a SAR?

A. Early withdrawal of funds [Your answer is partially correct.]
B. Termination of the insurance product accompanied by surrender charges. [Your answer is partially correct.]
C. The funds taken are directed to a third party [Your answer is partially correct.]
D. All of the above [Your answer is correct.]

AML Case Study: Insurance Sales through FINRA Broker-Dealer

John Perch, a well-established salesman, employed by a South Florida International Brokerage Services (SFIBS), a subsidiary of a Miami, Florida-based financial services firm, has lived in the Miami area for over 40 years. John is licensed to sell insurance products and securities. John's sizeable income allows him to engage in real estate investments in the area. His real estate investment activities have introduced him to many wealthy people, such as Thomas Charles, who have become clients of his securities firm.

Thomas Charles, unbeknownst to Perch, is not a U.S. citizen and is associated with a drug smuggling syndicate that finances terrorist activities in the Middle East. Charles was, in fact, listed by OFAC as a Specially Designated National (SDN). Charles, however, lived in Miami for over 20 years, rising to become a prominent real estate investor. Charles has no criminal record in the United States and has been a good neighbor to Perch.

Over drinks after their weekly tennis match, Charles tells Perch he had recently sold some properties that had netted him $100,000 in cash. Charles asked Perch if his firm could accommodate him. Perch, delighted, immediately said "yes" and scheduled a meeting at his office the following day in order to open an account for Charles.

Brokerage account opening

Since Perch had known Charles for so many years, he simply assumed Charles was an American citizen. For the account opening documents, Perch obtained the relevant information, such as name, date of birth, address, and customer identification number. The identification number Charles provided was that of a limited liability company (LLC). The LLC employed the services of a nominee

incorporation services (NIS) firm. The NIS firm provided the LLC with nominee officers, directors, and stockholders.

Charles told Perch he wanted to purchase a $5 million life insurance policy. Perch indicated to Charles that as a very wealth man with no children or immediate family, a $5 million insurance policy was not a suitable investment. Charles replied as a "key person" of the LLC whose customer identification he used, required him to purchase a life insurance policy in that amount. Perch then agreed and completed the insurance application form. Upon approval of the policy from the insurance company several days later, Charles returned to Perch's office to pay the first few premiums. Charles arrived with $20,000 in cash to cover the premiums, which were $10,000 each.

Perch told him that federal regulations required his firm to file a Currency Transaction Form for all currency transactions over $10,000. Charles declined. He said he would pay the premiums through the deposit of securities owned by the LLC and then he would take out margin loans in the amounts of $5000 on each premium due date and pay the balance of $5000 in cash.

Perch's manager approved of this arrangement because of the long-standing relationship with such a prominent client. Charles' firm did verify the customer identification number. However, the identification number should have sent up additional red flags because it was the number of a limited liability company. The LLC, a shell company, was licensed in the state of Florida. Since Charles was a well-known person in town, known to Perch and his manager, they did not consult OFAC to determine if Charles was on the list of "Specially Designated Nationals and Blocked Persons." Further, once they discovered the customer identification number was that of a corporation, they should have requested additional documentation.

Review

Did Perch properly open the account?
Yes
Your answer is incorrect. While Perch did record the proper information for a U.S citizen such as name, address, date of birth, and identification number, his client was not a U.S. citizen. Failure to determine this resulted in a further failure to secure acceptable customer identification documents for non-U.S. citizens, which are a taxpayer identification number; a passport number, an alien identification card number, or the number and country of issuance of any other government-issued document that bears a photograph of the customer. Perch failed to properly document Charles' identity. If he had, he would have realized the customer identity number was that of a shell corporation rather than that of an individual. Perch, had he done his job correctly, should have required Charles to supply the LLC's certified articles of organization.

No
Your answer is correct. While Perch did record the proper information for a U.S. citizen such as name, address, date of birth, and identification number, his client was not a U.S. citizen. Failure to determine this resulted in a further failure to secure acceptable customer identification documents for non-U.S. citizens, which are a taxpayer identification number; a passport number, an alien identification card number, or the number and country of issuance of any other government-issued document that bears a photograph of the customer. Perch failed to properly document Charles' identity. If he had, he would have realized the customer identity number was that of a shell corporation rather than that of an individual. Perch, had he done his job correctly, should have required Charles to supply the LLC's certified articles of organization.

Did South Florida International Brokerage Services (SFIBS) comply with OFAC regulations?
Yes
Your answer is incorrect. South Florida International Brokerage Services (SFIBS) did **not** comply with OFAC regulations. Broker-dealers and their employees must comply with OFAC regulations that prohibit transactions with persons and organizations listed on the OFAC website as "Terrorists" and "Specially Designated National and Blocked Persons". Had Perch or his manager checked the OFAC website as they were required to do under AML regulations, they would have discovered Charles was an SDN and he had dealings with embargoed countries.

No
Your answer is correct. South Florida International Brokerage Services (SFIBS) did **not** comply with OFAC regulations. Broker-dealers and their employees must comply with OFAC regulations that prohibit transactions with persons and organizations listed on the OFAC website as "Terrorists" and "Specially Designated National and Blocked Persons". Had Perch or his manager checked the OFAC website as they were required to do under AML regulations, they would have discovered Charles was an SDN and he had dealings with embargoed countries.

Continuing business relationship
Over the next five years, Charles continued conducting securities-related business with Perch and his firm. Charles would purchase additional securities such as mutual funds that he would pay for with checks drawn on the LLC. Every security he purchased would be sold within three months of its purchase date with the proceeds remitted to Charles. In addition, he withdrew the cash value of his life insurance policy, discontinued paying the premiums, and let the policy lapse. Three years later, Charles purchased another life insurance policy again paying the premiums of $10,000 with $5000 cash and $5000 with a check drawn on the LLC.

Charles maintained good relations with Perch and Perch's manager. Charles would often entertain them at his country club. Just as he was a model neighbor, he was also a model client. He never inquired about the performance of his securities and never complained about the high redemption fees for the early withdrawal from his mutual funds or cancellation fees from his insurance policy.

Perch's manager was also the designated compliance officer for his firm. During his testing of the firm's AML procedures, he noticed the frequent redemptions of the mutual funds and cancellation of the insurance policy. Since he knew Charles, and knew of his prominent position in town, as well as being a guest of Charles's at charity functions at Charles' country club, he thought it would be inappropriate to file a SAR report. Since there was no one else at the firm qualified to conduct independent testing, Perch's manager was the designated AML compliance person. Under compliance regulations of FINRA Conduct Rule 3310, Perch's manager is required to report his findings in the independent review to a senior person. The only person senior to the manager was the principal owner of the firm who was also a neighbor and friend of the client. The manager reviewed the firms AML procedures, controls, and training plans every three years and then submitted his review to the firm's owner.

Review

Does SFIBS need to file CTRs or SARs?
Yes
Your answer is correct. South Florida International Brokerage Services needs to file a SAR because the account and its activity have demonstrated several traditional red flags. Among those red flags are the client's lack of concern for commission or redemption costs and the appearance of structuring payments in currency of less than $10,000 in order to avoid the filing of a CTR. The use of an LLC shell company also requires heightened scrutiny. In addition, SFIBS should exercise special scrutiny because they are located in an area of high-risk of drug trafficking.

No
Your answer is incorrect. South Florida International Brokerage Services needs to file a SAR because the account and its activity have demonstrated several traditional red flags. Among those red flags are the client's lack of concern for commission or redemption costs and the appearance of structuring payments in currency of less than $10,000 in order to avoid the filing of a CTR. The use of an LLC shell company also requires heightened scrutiny. In addition, SFIBS should exercise special scrutiny because they are located in an area of high-risk of drug trafficking.

Are SFIBS's AML procedures adequate?

Yes
Your answer is incorrect. The AML procedures of SFIBS have many shortcomings.

No
Your answer is correct. Under the provisions of Conduct Rule 3310, SFIBS is required to conduct annual reviews of their compliance procedures. The annual review would have uncovered the fact that SFIBS did not have sufficient controls to discover the customer identification number was that of a corporation and not of an individual.

Second, the firm did not conduct sufficient verification efforts. Heightened scrutiny is required when the account identification number is that of a corporation; especially, if the identification number is a shell corporation employing a nominee incorporation services firm.

Once SFIBS discovered Charles was not a U.S. citizen, it should have verified his identity by requesting a passport number and country of issuance, an alien identification card number, or the number and country of issuance of any other government issued document that bears a photograph of the customer. Had they done so, they would have found Charles's true identity as a foreign national who had assumed many different names.

SFIBS was also in violation of Conduct Rule 3310 because it conducted comprehensive AML compliance reviews *every three years*. The rule requires *annual reviews*. Perch's manager as the designated AML compliance person clearly had a conflict of interest because he socialized with Charles. The manager did, however, report the findings of his compliance review to a person senior to him as is required by the rule.

Lastly, broker-dealers need to be aware of the money laundering opportunities available in mutual fund investments. Mutual funds have AML requirements similar to other financial institutions. Further, if SFIBS is the manager of the mutual funds Charles routinely redeemed early, it was required under the AML regulations to file a SAR because the redemptions would have set off a red flag.

Conclusion

Money laundering is a serious concern for our country. A number of state and federal laws, most notably the Money Laundering Control Act of 1986, the Bank Secrecy Act, and the USA PATRIOT Act, provide a strong arsenal of weapons in the fight against money launderers.

Banks, broker-dealers, insurance companies and other financial institutions have long been the subject of regulation to help law enforcement stem the tide against money laundering. The USA PATRIOT Act is important because it extends the reach of anti-money laundering to life insurance companies and requires life insurers issuing covered products to file SARs when customers or employees act suspiciously.

The Internal Revenue Service conducts AML compliance reviews. The examination procedures are similar to AML examinations in industries other than insurance.

Insurance companies should expect examiners to test four AML program elements required of insurance companies: internal controls, designation of an AML compliance officer, training, and independent testing.

Section Review

1. Fines and penalties for violations for failing to comply with AML Laws are assessed on a/an _____ basis.

A. Annual **Your answer is incorrect. Fines and penalties are not assessed on an annual basis.**
B. Weekly **Your answer is incorrect. Fines and penalties are not assessed on a weekly basis.**
C. Per Violation **Your answer is correct. These fines and penalties are assessed on a per violation basis, making it very expensive to avoid compliance or engage in money laundering activities.**
D. Case-by-case **Your answer is incorrect. Fines and penalties are not assessed on a case-by-case basis.**

2. Officers, directors and employees of financial institutions may face how many years of imprisonment for engaging in transactions involving money laundering?

A. 10 **Your answer is incorrect. Officers, directors and employees do not face 10 years imprisonment.**
B. 15 **Your answer is incorrect. Officers, directors and employees do not face 15 years imprisonment.**
C. 30 **Your answer is incorrect. Officers, directors and employees do not face 30 years imprisonment.**
D. 20 **Your answer is correct. Parallel fines, penalties, and sanctions can be applied personally to officers, directors, and employees of financial institutions. The federal penalties for engaging in transactions involving money laundering, assisting with money laundering, or structuring a transaction to avoid a BSA or other reporting requirement include the following: 20 years imprisonment; fines up to two times the amount of the laundered transactions or $500,000, whichever is greater; and, additional civil fines for violating other laws and regulations.**

3. Failing to file a report required by the BSA or filing a false or fraudulent report could result in imprisonment of up to how many years?

A. 5 **Your answer is correct. Fines of up to $500,000 and five years imprisonment can result from the following types of crimes: Failing to file a report required by the BSA; or filing a false or fraudulent report required by the BSA.**
B. 10 **Your answer is incorrect. This does not result in imprisonment of 10 years.**

C. 20 **Your answer is incorrect. This does not result in imprisonment of 20 years.**
D. 30 **Your answer is incorrect. This does not result in imprisonment of 30 years.**