



NATIONAL ASSOCIATION OF INSURANCE AND FINANCIAL ADVISORS – FLORIDA

1836 Hermitage Blvd, Suite 200, Tallahassee, FL 32308

Contact: Paul S. Brawner

(850) 422-1701

brawner@faifa.org

This self-study course is approved by the Florida Department of Financial Services for continuing education credit. Provider is the National Association of Insurance and Financial Advisors – Florida (#654). Course is approved for two (2) hours of credit, intermediate level, for course authority 2-15. Course ID # is 77098.

HERE'S HOW IT WORKS: Read the following article and when you're ready to take the exam, simply contact Paul S. Brawner at brawner@faifa.org and request the exam. You'll receive the exam and an affidavit attesting you did not receive help on the exam. Return the exam and signed affidavit via fax, e-mail or regular mail (see contact information at top of page). Upon successful completion of the exam (70% or higher), NAIFA–FL will send you a Certificate of Completion within 20 business days.

ANTI – MONEY LAUNDERING

2 Hours of Self-Study CE

Course Reading Assignment

The goal of this course is to help insurance agents, financial advisors and company employees better understand the anti-money laundering program and more fully appreciate the role they play in its success. This course explains and discusses the risks, methods of detection and consequences of money laundering in the insurance and financial services industry. Special attention is given to the role producers and employees play in their company's AML program and details some best practice ideas to provide a better understanding of AML responsibilities.

I. INTRODUCTION: WHAT IS MONEY LAUNDERING AND ANTI-MONEY LAUNDERING?

Money Laundering

If you ask most agents and agency employees, they'll tell you they understand that money laundering is illegal. But not everyone knows what money laundering really means. Financial professionals who sell life insurance and annuities must understand not only what this term means but the consequences it carries, because these products are surprisingly popular tools in the world of money laundering.

Simply put, money laundering is the act of combining illegally obtained money into the legal monetary system in so that it hides the illicit origins. The reason for this is simple: dirty money that isn't "laundered" leaves an audit trail that can be traced. Money that has gone through a "wash cycle" will seem legitimate and can be used without scrutiny.

Following the September 11 terrorist attacks the government learned that laundered money financed some of the pre-attack preparations by terrorists. While there isn't any evidence that insurance products were used for this purpose, other high-profile criminal cases have involved life insurance policies and annuities in money laundering schemes.

There's a price to pay for this service, because by the time an illicit dollar completes a laundering process it may be worth far less than its original value. Still, money laundering can be a lucrative business for those in a position to assist in the process. Most participants are fully knowledgeable of their actions in the process. Others are not, such as an insurance agent or financial advisor who sells a life insurance policy under unusual circumstances without checking deeper. Regardless of whether an individual knowingly or unknowingly participates, the common denominator in all cases is money. Criminals know this all too well, and are willing to pay very well to cleanse their ill-gotten gains.

Anti-Money Laundering (AML)

AML refers collectively to laws, policies, and company programs intended to detect and/or deter money laundering. It is, simply put, the opposite of money laundering. Opposing the criminal and terrorist elements that would launder money are various anti-money laundering forces, consisting of government, law enforcement, and business. These entities, using federal regulations like the USA PATRIOT Act, have become an important element of US national security. If you weren't already aware of it, insurance institutions and those who represent them are included.

SECTION REVIEW – QUESTION 1

Which of the following **IS NOT** terms associated with the collective definition of AML?

[Section I, Page 2]

- a. Laws
- b. Company programs
- c. Practices
- d. Policies

SECTION REVIEW – QUESTION 2

Which of the following is the correct description of money laundering?

[Section I, Page 2)

- a. Dirty money that is “laundered” so it leaves an audit trail that can be traced
- b. Integrating illegally obtained money into a legal monetary system to hide the illicit origins
- c. Intentionally detecting and/or deterring money laundering
- d. Money put through a “wash cycle” that can legitimately be spent or invested freely

II. HISTORY

No one can be certain as to when money laundering first began. However, there is considerable evidence that it's been going on for several thousand years. Over that span of thousands of years people have used money laundering techniques to move money resulting from crime - but also often to hide and move it out of reach of governments - including oppressive regimes and despotic leaders.

If it were only limited to money laundering, the government likely would have little interest in getting involved in the issue. Federal agencies like the Treasury Department and the Federal Bureau of Investigation (FBI) have investigated money laundering for decades, but the issue grew to its current status on September 11, 2001.

One noteworthy event, known as Operation Capstone, clearly illustrates the risk that insurance companies face in money laundering schemes. While there's no evidence that the money laundered through insurance companies in the Capstone case funded terrorist activities, it easily could have. In 2002, a sophisticated international money laundering operation was exposed in which life insurance companies in the United States, Great Britain, and other locations around the globe were used to launder some \$80 million worth of Colombian drug proceeds over a three year period. A two-year investigation revealed that Colombian drug trafficking organizations, through a small number of insurance brokers, were buying high-premium cash value life insurance policies in the United States, Great Britain, and other locations. These policies were purchased with tens of millions of dollars' worth of drug proceeds sent to insurance companies by third parties around the globe, via cashier's checks and wire transfers.

Operation Capstone revealed that owners were heavily funding their policies just shy of MEC levels to avoid IRS scrutiny and making early withdrawals to access the cleansed money within. Changes in policy ownership were common. Substantial contract penalties were assessed for early withdrawals and surrenders, but these charges were probably viewed by those involved as a normal cost of doing business.

The policyowners, all associates of several Colombian drug cartels, would receive checks or wire transfers from the insurance company that, on their surfaces, appeared to be legitimate insurance proceeds. The laundered money was now available to fund any purpose that served the cartel's interests.

As this case showed, the existence of insurance company AML programs offers little or no protection if the programs are not supported by active compliance enforcement. Operation Capstone demonstrated that insurance companies, like other financial institutions, are susceptible to money laundering and proved that Congress was right to include insurance companies in the mandates set forth in the USA PATRIOT Act.

SECTION REVIEW – QUESTION 3

Operation Capstone revealed that owners were heavily funding their policies, just shy of MEC levels. What was the reason for this?

[Section II, Page 3)

- a. To avoid IRS scrutiny
- b. To avoid taxation
- c. To maximize the amount of return on their investment
- d. Because the FBI only monitored purchases above the MEC level

III. THE MONEY LAUNDERING PROCESS

There is no single way to launder money. Rather, the process involves any series of financial transactions that moves cash or other assets from one location to another, or from one form to another, in such a way as to hide its origins and, in the end, make the money appear legitimate. While there are countless variations on the theme, money laundering generally involves three stages: placement, layering, and integration.

Placement

The first stage in the money laundering process is **placement**. Placement brings the illicit cash into the legal financial system, and is intended to obscure the start of any audit trail. This process involves avoiding financial accounts or products that record ownership. This cover-up is typically achieved by converting cash into equivalent instruments like cashier's checks, money orders, traveler's checks and wire transfers.

Layering

To further hide the trail from its illicit source, the second stage of the money laundering process, known as **layering**, is begun. Here cash equivalents obtained in the placement stage are now used to purchase different financial instruments. However, simply exchanging cash for money orders

and then depositing them into a personal bank account does little to hide the link between the criminal and the crime. Instead, the cash equivalents are used as premiums and deposits for more sophisticated financial products that provide liquidity and, more important, distribute or disburse funds in a manner that appears fully legitimate. Sophisticated financial products can include cash value life insurance and deferred annuity contracts. Depending on the level of the money laundering operation, insurance policies purchased with tainted cash equivalents may be quickly surrendered or held for longer periods of time. Those that are held for longer periods frequently experience changes of ownership.

Integration

We now enter the last stage in the money laundering process – **integration**. Here, the “cleansed” money is circulated back into the hands of the criminal and ultimately into the financial system. Like clothes that have completed a wash cycle, money that has cycled through the placement and layering process is clean and ready to be used again. It can be invested quietly or flashed in public. Any questions as to its source can be addressed with a legitimate answer.

SECTION REVIEW – QUESTION 4

Which of the following is **NOT** a legitimate stage in the money laundering process?

[Section III, Page 4-5)

- a. Layering
- b. Placement
- c. Integration
- d. Laundering

IV. INSURANCE IN THE MONEY LAUNDERING PROCESS

At first thought, you might not think that insurance contracts would be attractive to money launderers. Obviously, underwriting requirements would put the buyer and potential insured under a microscope, and most insurance products carry policy fees, insurance charges, and surrender penalties that would reduce the contract’s value.

Upon closer look, however, it’s really not difficult to understand how these products could in fact serve as an ideal tool for “cleansing” illicit funds. Cash value life insurance and deferred annuity contracts provide owners access to funds through policy loans, partial withdrawals, or outright surrenders. Free-look surrenders are especially attractive because they avoid surrender charges, even though the prospect of paying a surrender charge is not a serious deterrent to those laundering money. In fact, such fees are deemed a reasonable business expense for the privilege of accessing contract values on demand. Regardless of how the money is received from the policy

or contract, the common denominator is the insurance check that gives the payment legitimacy. Any funds obtained this way will appear fully legal and can be sent or wired anywhere.

To see the potential role life insurance can play in money laundering, consider the following:

A financial services broker is exceeding his wildest sales goals, all because of one person. Andre, a customer who walked into the agency a year ago asking to buy a \$500,000 universal life insurance policy. Andre was a 45-year-old computer technology business owner who wanted the policy for business purposes. It wasn't long before the agent was writing large cash value policies on business associates and personal friends. The link in every case was the buyer's interest in the policy's living benefits. If there was a way to use cash value life insurance to accumulate future wealth, Andre wanted to know.

The agent was now busy serving the insurance needs of his select clientele. However, it wasn't long before the agent noticed some puzzling tendencies: frequent withdrawals, partial surrenders, cancellations during the free-look period, etc. Also, policy distributions were directed to off-shore bank accounts. These events gave some concern to the agent, and drew occasional questions from the home office, but with sales continually the agent on top of the agency's leader board, the questions were not followed up.

Premiums for these policies were occasionally paid in person, usually by courier and always with money orders, but they were most frequently paid by wire transfers from banks in several different countries. Since Andre's business involved business dealings with companies in other countries, it seemed to make sense he would have accounts in banks around the world. And he deduced that doing business through an off-shore bank is an excellent way to reduce taxes, if not avoid them entirely. That certainly wasn't illegal. Any reasons to suspect Andre's money sources weren't recognized by the agent. By now, the commissions he was earning were so good the last thing on his mind was questioning where the money was coming from.

What the agent didn't know was that almost all the money used to purchase the policies and contracts was gained through illicit drug trafficking. Andre was involved with an international drug cartel and were laundering millions of dollars generated annually from cocaine and heroin sales. The volume of cash involved was staggering, and no cartel member could spend or save this amount of money without drawing inquiries. The money could only be used if it was shuffled around and made to reappear as legitimate money.

The money laundering operation set up by Andre and his associates followed the standard three-stage process characteristic of most money laundering schemes:

- **Placement** occurred when the cash was deposited into off-shore bank accounts, where it was subsequently wired to the agent's insurance company to pay premiums

- **Layering** was achieved through buying multiple life insurance and deferred annuity contracts using cash payments and wire transfers from uncertain sources. Ownership changes helped cover any audit trail.
- **Integration** occurred through partial surrenders and withdrawals in the form of insurance company checks, which moved the money back into the legal monetary system.

Other Possible Scenarios

There are many ways in which life insurance can be used to launder money. For example:

- A life insurance policy could be purchased and then cancelled during the free-look period to receive a refund of the premium. The returned premium is used to purchase other assets or investments, thus adding layers to the process and further integrating the money into the financial system.
- A life insurance policy could be purchased and the policy values used as collateral for a loan to buy real estate. The loan is repaid by surrendering the policy, and the launderer now owns property that can be retained or sold at a later date.

SECTION REVIEW – QUESTION 5

Insurance or annuity products have features that make them excellent tools for “cleansing” illicit funds. Which of the following is **NOT** one of those features?

[Section IV, Page 5)

- a. Intrinsic value
- b. policy loans
- c. partial withdrawals
- d. outright surrenders

V. REGULATORY BASIS FOR ANTI-MONEY LAUNDERING

Federal anti-money laundering laws have evolved over the past several decades, with the modern era of AML regulations beginning in 1970 with the enactment of the Bank Secrecy Act. The law that impacts insurance companies the greatest, the USA PATRIOT Act, is a direct descendant of that law.

Bank Secrecy Act (BSA)

Created in 1970, this is widely considered the first significant federal AML law in the US, and established the requirement that financial institutions report large deposits of cash. It was initially directed only at banks, and required financial institutions to help create an audit trail by keeping records and reporting cash (or cash equivalent) transactions exceeding \$10,000.

Information provided through BSA compliance is used by domestic and international enforcement agencies to identify and prosecute money laundering. The BSA's most notable requirements include the following:

- Cash payments over \$10,000, received in a trade or business from one buyer, must be reported to the IRS using Form 8300
- Businesses and individuals that own foreign bank accounts, brokerage accounts, mutual funds, unit trusts, or other financial accounts in which the aggregate value exceeds \$10,000 are required to report the account annually to the IRS
- Banks must file a Suspicious Activity Report (SAR) for any suspicious transaction relevant to a possible violation of law or regulation

These requirements are especially important to note because they form the basis of the current federal law dealing with money laundering and terrorism funding found in the USA PATRIOT Act.

The USA PATRIOT Act

In the days and weeks following the September 11, 2001 terrorist attacks, Congress focused on reducing or eliminating weaknesses in the US economic system that may have contributed to that event. Barely a month later Congress passed the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001**. Of course, this long phrase is better known by its acronym, the USA PATRIOT Act. It was signed into law on October 21, 2001 and among its provisions it amended some of the rules of the Bank Secrecy Act and extended them to nonbank financial institutions, including insurance companies and brokerage firms. Also, the act increased the ability of law enforcement agencies to search electronic communications and medical, financial, and other records. As it relates to the insurance industry, it expanded the Treasury Department's authority to regulate financial transactions, particularly those involving foreign individuals and entities.

Actually, the focus of the USA PATRIOT Act was not necessarily on money laundering, but rather on any financial transaction that might be connected to terrorist financing. Specifically relevant to the insurance industry is Title III of the PATRIOT Act. This section addresses money laundering and expands the Bank Secrecy Act to include all financial institutions, including life insurance companies.

The USA PATRIOT Act's inclusion of insurance companies recognized the simple fact that some insurance products were being used in money laundering schemes. Criminals will use any financial instrument that provides liquidity to clean dirty money. As banks became less accessible for their needs (thanks to the 30-year-old Bank Secrecy Act), money launderers' attention turned to deferred annuities and cash value life insurance.

SECTION REVIEW – QUESTION 6

Which federal AML law established the requirement that financial institutions report large deposits of cash and create audit trails of transactions exceeding \$10,000.

[Section V, Page 7)

- a. Terrorist Act of 2001
- b. USA PATRIOT Act
- c. Bank Secrecy Act
- d. Suspicious Activity Reporting Act

VI. FINCEN FINAL RULES

The USA PATRIOT Act intended from the start to include insurance companies in the definition of “all financial institutions.” The nature and complexity of insurance products made it apparent that additional guidelines were needed to define how insurance carriers should comply with AML requirements.

In November 2005 the Treasury Department’s **Financial Crimes Enforcement Network (FinCEN)** published some final rules geared specifically towards insurance carriers:

- Insurance companies be required to develop and implement anti-money laundering programs
- Insurance companies be required to report suspicious transactions

Establish a Risk-Based Anti-Money Laundering Policy

As a result of the FinCEN rule the insurance companies now had to establish and implement a risk-based anti-money laundering program. “Risk-based” meant the company’s AML program had to reflect the unique money laundering risks it faced. The intent was to prevent a company’s “covered products” (mainly cash value life insurance and deferred annuity contracts) from being used in money laundering or terrorist activity financing.

Report Suspicious Transactions

The second FinCEN final rule amended the Bank Secrecy Act of 1970 to include insurance companies in the list of those that are required to report “suspicious activity” involving certain covered product transactions through the filing of a suspicious activity report (SAR).

Both of the above rules are detailed later in this course.

VII. AML RULES FOR INSURERS

Earlier we made it clear that there is a definite role for certain types of life insurance and annuity contracts in money laundering activities – including terrorist financing. So it should be entirely understandable that these products are included in anti-money laundering laws. This section will take a closer look at what insurance companies must do to comply with the USA PATRIOT Act’s

requirements. The emphasis is on companies' roles and responsibilities, but there is a direct relevance to producers for a reason: producers are central to every insurer's AML policies and procedures.

Insurance Company Obligations under the PATRIOT Act

As addressed in the FinCEN final rulings, the USA PATRIOT Act requires financial services companies involved in the sale of "covered products" to comply with the following:

- Designate a compliance officer to oversee the company's development and implementation of AML policies and procedures
- Develop and maintain internal policies, procedures, and controls to help identify and report potential money laundering transactions
- Maintain an ongoing training program for all associates who are involved in any sale and administration of "covered products"
- Maintain independent audit procedures to periodically test the AML policies and procedures

AML Rule Regarding Covered Products

It's important to note that not all AML rules apply to all insurance companies or all insurance products. They are directed specifically at companies that sell **covered products**, which are defined as the following types of life insurance and annuity contracts:

- individual permanent life insurance (including whole life, universal life, variable life, and any other product that builds cash value)
- individual annuities (fixed or variable, immediate as well as deferred)
- any other insurance product that includes a cash value or investment component

Products that do not provide the liquidity essential to money laundering are not covered by the PATRIOT Act. This distinction means that any product that does not include an internal cash value is not covered under the act. Term life insurance (individual as well as group insurance) is a good example. Though term life insurance can be used in a money laundering operation – for example through free-look surrenders – the cash value element of permanent life insurance presents a far more liquid source of laundered cash than term. This makes it far more likely to be used. Thus, permanent life insurance is a "covered product" under the USA PATRIOT Act.

Excluded from the definition of "covered products" are group life insurance or group annuity products of any type, as well as the following:

- Term, credit life, property, casualty, liability, health, and title insurance
- Indemnity contracts and structured settlements (including worker compensation payments)
- Products offered by charitable organizations, such as charitable annuities
- Reinsurance and retrocession contracts

Designate an AML Compliance Officer

One of the first steps in creating an AML policy is to designate a compliance officer whose responsibility it is to oversee the policy's development, and then ensure its effective implementation and maintenance. The compliance officer is responsible for the day-to-day operation of the company's AML program and for ensuring that the requirements or steps laid out in the program are fully implemented and followed.

Develop AML Policy and Procedures

The USA PATRIOT Act requires that financial institutions create and maintain policies, procedures and controls to identify and report potential money laundering transactions. A company's AML program is published in a written policy document that must be made available to the Treasury Department or FinCEN upon request.

Each company's policy will probably vary, but common topics addressed in the AML policy document would include the following:

- A statement of policy and principles. This document declares that the policy is developed in compliance with the USA PATRIOT Act of 2001. It will identify an AML Compliance Committee, usually consisting of the company's chief compliance officer, general counsel, and other compliance, finance, and accounting officers.
- Statement of scope – This policy statement usually includes a provision identifying company associates who are subject to the policy. Typically, it includes all employees, officers, and appointed producers.
- List of covered products – This statement would include a description of the products covered under the AML policy, and should align with FinCEN's definition of covered products.
- Customer Identification Program
- Monitoring and reporting – Most companies engage in *transaction-based monitoring*, simply meaning all transactions involving covered products are monitored. Those that match certain criteria or raise a "red flag" will be documented and possibly reported to FinCEN using the Suspicious Activity Report (SAR).
- Investigation – This section would require that if suspicious activity is detected, the company's AML Compliance Committee will begin an investigation to determine whether a report (SAR) should be made to appropriate law enforcement or regulatory agencies..
- Record-keeping – This section will detail requirements for maintaining information provided by the customer. The standard requirement is that it must be recorded and maintained for five years after the customer's account is closed or policy surrendered.

Ongoing AML Training

Criminals will always look for new ways to launder money, so insurance and financial services companies must continually revise their AML programs. That includes the training it provides. To stay current with their company's AML programs, producers need to continually update their knowledge. The practical way to do that reliably is through training.

The USA PATRIOT Act requires that companies "maintain an ongoing training program." Most companies have interpreted this requirement to mean an annual education requirement for producers and employees involved in the sales or servicing of covered products. The PATRIOT Act doesn't specifically outline the curriculum a training program must follow, but the rules do state that companies may satisfy this requirement by training their producers directly or through a third party. The training may be provided in a classroom environment or through online media.

Topics that are typically covered in a company AML training program include the following:

- definitions and examples of money-laundering, terrorist financing, and AML strategies; and
- producer responsibilities with respect to:
 - methods of payment
 - identifying red flags and reporting suspicious activity
 - collecting relevant customer information and "knowing the customer"
 - record-keeping
 - generally knowing and complying with the company's AML requirements

Periodic AML Testing

To detect suspicious activity, insurance and financial institutions use a screening process to spot certain "markers" that may require a closer look. A marker is any specific policy or contract activity the compliance department deems subject to scrutiny. A company may feel confident that its AML program is working if it periodically detects these markers, but is it catching every instance of money laundering?

To determine if the AML program is effective and to look for breakdowns in the process, companies are required by the USA PATRIOT Act to periodically test their programs using an independent third party, such as an outside auditing firm. Independent auditing firms challenge an insurance company's AML program by periodically attempting transactions involving covered products that should trigger a red flag. In many instances, these tests will involve the company's agents and brokers. The company's response to the test is reported to its AML compliance committee for review and appropriate action.

Develop and Implement a Risk-Based Assessment

FinCEN requires insurance companies to develop a risk-based AML program that is based on the company's assessment of the money laundering and terrorist financing risks associated with its covered products. The basis for a risk-based AML policy can be traced to the Bank Secrecy Act of

1970. Under the BSA, financial institutions are required to “identify, assess, and mitigate” the money laundering risks they face.

This requirement gives companies latitude in designing an AML policy that fits their unique profiles, taking into account a company’s jurisdiction, products and services, and clients. As such, a company must assess the money laundering risks it faces that relate to the following:

- The companies’ covered products and the provisions in those products (i.e. surrender provisions, policy loan limits, etc.)
- How company products can be purchased (i.e. cash versus checks)
- Demographic profiles of customers, especially those who are nonresident aliens, privately held corporations, small businesses, and charitable organizations
- The company’s distribution channels, especially those involving independent producers and international entities
- The company’s transactions processes, notably those dealing with how producers transmit customer premiums and deposits to the company
- The company’s international presence

Customer Identification Program

A very important AML rule is “Know the customer.” In addition to obtaining basic information required by the company, this rule includes the responsibility to be alert to strange or unusual behavior and requests made by the customer.

Section 326 of the USA PATRIOT Act requires that financial institutions establish a **customer identification program (CIP)**. At a minimum, companies must identify the following customer information:

- Full legal name
- Social Security number or tax identification number
- Date of birth
- Residential address

Companies must determine, within a reasonable period after an account is opened or a policy is purchased, if the applicant’s name appears on a list of known or suspected money launderers, terrorist organizations, and other criminals maintained by the Treasury Department’s Office of Foreign Assets Control (OFAC). This list is more commonly known as the **Specially Designated Nationals and Blocked Persons** list.

As part of a CIP program, a Notice to Customer statement must be given to every applicant for a covered product. The purpose of a Notice to Customer is to disclose the company’s intent to verify the customer’s name and personal information. Applicants who refuse to provide personal information will be declined.

SECTION REVIEW – QUESTION 7

Which of the following types of life insurance and annuity contracts are defined as **covered products**?

[Section VII, Page 10)

- a. Corporate Individual permanent life insurance
- b. Group life and annuity products
- c. Individual annuities (fixed or variable, immediate as well as deferred)
- d. Any finance contract that includes an investment component

SECTION REVIEW – QUESTION 8

Topics that are typically covered in a company 's producer AML training program include all of the following **EXCEPT**

[Section VII, Page 12)

- a. methods of payment
- b. identifying red flags and reporting suspicious activity
- c. commission amounts on different covered products
- d. collecting relevant customer information and "knowing the customer"

VIII. AGENTS AND BROKERS

Insurance agents and brokers are not required to have separate anti-money laundering programs. The insurance company must devise and maintain AML policies and programs. However, because agents and brokers are an integral part of the insurance industry they have an important role to play in assisting the insurance company in its anti-money laundering efforts. Agents and brokers are in the critical position of knowing the source of investment assets, the nature of their clients, and the objectives for which the insurance products are purchased. As such, each insurance company must enroll its agents and brokers into its anti-money laundering program and monitor their compliance with the program. The insurer is ultimately responsible for the conduct and effectiveness of its anti-money laundering program, which includes the activities of the agents and brokers who are involved with covered products. Insurers must exercise due diligence, not only in the development of their AML programs and in the collection of appropriate customer and other information, but also in monitoring the operations of their employees and producers.

By now, every insurance company that sells covered products has a formal AML policy in place. While the PATRIOT Act puts the burden for creating an AML program on the shoulders of

insurance companies, the producers' front-line position puts agents and brokers at the heart of every company's AML policy.

Producer and Employee AML Responsibilities

We now need to take a closer look at the role employees and producers play in an insurance company's AML program. It is vital that insurance and financial professionals understand the relationship they have with their insurance company's AML program, know what they must do to fully comply, know how to detect money laundering red flags, understand the company's process for investigating and reporting suspicious activity, and integrate their companies' suspicious activity reporting requirements into their practices.

An insurer's AML program depends heavily on its employees and producers, whom they rely on to be aware of the realities of money laundering, to be knowledgeable of their AML programs, and to be committed to using compliant AML business practices. The producer's role in the core requirements of current federal AML regulations includes the following:

- Obtaining and verifying an applicant's personal information
- Monitoring transactions and reporting suspicious activity
- Investigating
- Periodic testing

Detecting Red Flags

The cooperation of an insurance company's agents and brokers is important in all aspects of its AML policy, but none more so than in detecting red flags. A red flag is any fact, circumstance, or customer request that is unusual or simply suspicious. It might be the customer's request to make a partial surrender from a recently purchased life insurance policy, in spite of substantial surrender charges, with no apparent reason for the withdrawal. A withdrawal might also raise a red flag if the surrender check is directed payable to an apparently unrelated third party.

As a company's first point of contact with new customers, producers are uniquely positioned to detect red flags. Even an applicant's manner in answering application questions, something only the producer might observe, could raise a red flag. To help detect and report red flags, producers (and employees) must:

- Be alert for circumstances that don't quite make sense
- Ask follow-up questions to verify answers that seem unclear, unusual, or unexpected
- Be prepared to decline applications from persons who will not or cannot comply with requests for identifying information
- Be alert to vague or evasive responses to questions about the intended reason for purchase or use of the product
- Record notes of all conversations and observations

- Report all red flags to managers or field compliance principals as directed by the company's AML process. Concerns or suspicions are not to be discussed with the customer nor should the producer contact federal authorities directly

Red Flag Examples

Even though FinCEN cited a number of red flag examples in its 2005 final rules, the list is not all-inclusive. The techniques of money laundering are continually evolving and there is no way to provide an exhaustive list of suspicious transactions. Red flags can generally be separated into three categories:

- new business
- premium and deposit payments
- policy activity

The geographical location of the parties involved in an insurance transaction can also raise the need for heightened awareness or increased scrutiny.

New Business Red Flags

Red flags to watch for during transactions involving the sale and issuance of new business include the following:

- Purchase of an insurance product that appears to be inconsistent with his or her needs
- Funds used to purchase product is inconsistent with customer's financial situation or profile
- Customer is reluctant to provide identifying information when purchasing an insurance product, or the customer provides minimal or seemingly fictitious information
- Customer exercises the "free-look" privilege shortly after the policy is issued
- Exhibiting unusual concern with government reporting requirements, especially those requiring personal identification information
- Applicant wishes to engage in a transaction that lacks business sense or apparent investment strategy or is inconsistent with the applicant's stated business strategy
- Applicant has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations
- Applicant lives in distant location and comparable policy can be purchased where he/she lives
- Applicant appears to be acting as an agent for an undisclosed party or principal, but is reluctant or refuses to provide information about them
- Applicant provides inconsistent answers to questions or misleading information
- Customer shows little or no concern for the investment performance of an insurance product but much concern about its withdrawals and surrender provisions
- Applicant exhibits lack of concern for policy fees and charges, especially early surrender fees
- Applicant is rated but shows casual disregard for higher premium he/she will pay due to rating

Premium and Deposit Red Flags

Red flags associated with premium and deposit payments include the following:

- any unusual method of payment, particularly by cash or cash equivalents
- payments received from unrelated third parties
- payments made through wire transfers of sizable amounts
- insurance product purchased with monetary instruments in a structured settlements
- the purchase of an insurance policy with numerous checks drawn on different accounts
- large payments that are followed closely by requests for partial surrenders or policy loans

Policy Activity Red Flags

Many policy transactions, such as a change in policy dividend options, are a normal part of insurance transactions and insurance business. Red flag activities are any that are unusual or atypical. Examples include the following:

- Early termination of an insurance product, especially at a cost to the customer or where cash was tendered and/or the refund check is directed to an apparently unrelated third party
- Lack of concern or questions about surrender charges when requesting a policy surrender
- Transfer of policy ownership to an apparently unrelated third party
- Borrowing the maximum amount available in the policy soon after its purchase
- Pattern of recurring policy loans with prompt repayments
- Payment of unscheduled premiums, followed shortly by one or more policy withdrawals
- Any request that a transaction be processed in a manner such as to avoid normal documentation or normal procedures.

Producer and Employee Red Flags

It shouldn't surprise anyone that not all red flags come from the customer transactions. Some are raised by suspicious activity demonstrated by the producer or a company employee. Usually they relate to a change in the producer's sales activity or employee's behavior. The change may be observed by a manager, a field compliance principal, or a compliance officer. However detected, the matter needs to be brought to the company's chief compliance officer or AML Compliance Committee. There may well be valid reasons for observed changes, but those would be determined only after a compliance review. The following are examples of activity that suggests a need for closer review:

- Agent has been an average producer in the agency for the past five years. However, she suddenly (and unexpectedly) exhibited a dramatic increase in sales, especially with limited premium permanent life insurance policies. Many of those policies have experienced frequent loans and withdrawals.
- An employee has always lived a modest, comfortable lifestyle. In the past several months, he has been spending money like there's no tomorrow, from major home improvements and a new car to dining out frequently and taking expensive vacations.

- An agent anxiously asks compliance department employees what they may know about cases being reviewed by the company's AML compliance committee.
- A broker has been writing a large number of policies for customers who live away from her normal business market, and quite a few have been returned during the free-look period.

Willful Blindness

It can be tempting to overlook a questionable premium payment, especially one involving thousands of dollars, but producers are not excused from AML compliance and reporting requirements on the pretense they didn't detect anything out of the ordinary. The legal concept of willful blindness — the intentional avoidance of knowledge of a crime to avoid civil or criminal liability for one's role in it — can subject an agent, advisor or broker to prosecution even if the person claims to have been unaware of suspicious activity.

Penalties

Whether through willful blindness or deliberate participation, anyone convicted of involvement in money laundering faces huge fines (up to \$250,000) and up to 20 years in prison for each transaction. These penalties include employees and appointed producers of insurance companies.

SECTION REVIEW – QUESTION 9

[Section VIII, Page 16)

Which of the following is **NOT** a category of FinCEN Red Flags?

- a. New business
- b. Policy activity
- c. Customer information collection
- d. Premium and deposit payments

IX. SAR RULES AND REQUIREMENTS

An insurance company's AML compliance policy is meaningless if the company doesn't actively maintain a process for detecting, reviewing, and reporting **suspicious activity**. The USA PATRIOT Act devotes considerable attention to this important element of anti-money laundering. Producers have a crucial role to play in the process of identifying and reporting signs of suspicious activity. This section details the AML rules and responsibilities dealing with the detection and reporting of suspicious activity. It's vital that the agent or advisor fully appreciate the crucial role they play in helping their companies detect suspicious activity, understand their companies' suspicious activity reporting requirements, and recognize red flags in any transaction, especially those involving covered products.

Detecting Suspicious Activity

The requirement that certain financial institutions report suspicious financial transactions to federal authorities extends back to 1970 and the Bank Secrecy Act. Until the September 11 terrorist attacks, insurance companies were generally exempt from these requirements. However, the PATRIOT Act requires insurers to identify and report suspicious transactions to FinCEN through the use of a **Suspicious Activity Report** designed for **Insurance Companies (SAR-IC)**.

Suspicious activity reporting required of insurance companies and other financial institutions reflects a simple reality: they are more likely than law enforcement to know when or if a financial transaction is not quite what it appears to be. Those closest to the business are better able to evaluate when a given purchase or transaction lacks legitimacy in connection with the products or services the company provides.

SAR Reporting: A Component of the Risk-Based Compliance Process

An effective anti-money laundering program uses a risk-based compliance process for identifying and reporting suspicious activity. As explained previously chapter, “risk-based” simply means that the company’s AML program reflects its unique set of money laundering risks: its covered products, distribution system, clientele, and jurisdiction. This arrangement, tracing back to the Bank Secrecy Act of 1970, requires financial institutions to engage in risk-based compliance that focuses compliance resources where the money laundering risk is greatest.

Transaction Monitoring

A key part of every company’s AML compliance program is its **transaction monitoring process**. This is the starting point for the screening that is the basis of AML compliance. Transactions may be monitored manually by employees and compliance principals as part of the company’s review escalation process, or they may be monitored automatically using computer systems that identify transactions displaying red flag characteristics.

Threshold Amount

While transactions involving any amount of money may be used in a money laundering scheme, the nature of the crime is such that money laundering almost always involves larger sums. One method of risk-based compliance is applying a payment threshold that separates transactions into two groups: those that require extra AML attention and those that do not.

Under FinCEN rules, the suspicious activity review threshold is **\$5,000**. Any covered product transaction that includes a payment (or aggregate of payments) of \$5,000 or more requires a closer evaluation by the company to assess the need to file an SAR-IC. Transactions may include cash value transfers between policies and 1035 exchanges as well as premium payments and deposits. Transactions exceeding the \$5,000 threshold are not necessarily reported to federal authorities. Instead, this threshold triggers a closer review by the insurance company’s AML compliance committee. If suspicious activity is detected, the company will report the case to

FinCEN. By the same token, transactions below the \$5,000 threshold may be (and should be) reported if they are suspicious or if they appear to violate the law.

The \$5,000 FinCEN threshold should not be confused with the longstanding requirement, from the BSA of 1970, that financial institutions report *all* cash payments exceeding \$10,000. FinCEN expects that two conditions will occur to mandate filing an SAR-IC:

- an aggregate of at least \$5,000 in funds or other assets
- facts or circumstances of the case that raise suspicion

On that latter point the rules state that a determination as to whether a SAR-IC report should be filed must be based on all the facts and circumstances relating to the transaction and customer. Different fact patterns will require different judgments. In describing “facts and circumstances” that may indicate a suspicious transaction, FinCEN uses the term “red flag”, which we learned is any fact or circumstance that is outside the customer's typical actions, especially where the economic gain is not obvious or clear. Companies (and the producers who represent them) must watch for red flags in all aspects of a covered product’s sale and servicing.

Reporting Suspicious Activity

A producer or employee who detects a red flag or any other suspicious activity is only required to report the suspicion to a manager or designated compliance principal. He or she should never discuss the concerns with the customer. The company’s AML process will escalate the case through several layers of compliance review before deciding if the activity will be reported to FinCEN. The insurance company’s compliance officer, not the producer, reports the case to federal authorities.

Suspicious Activity Report: SAR-IC

Suspicious activity is reported by the insurance company (not the agent or broker) to FinCEN using Form SAR-IC (Suspicious Activity Report by Insurance Companies). Any suspicious transaction *may* be reported, but those that exceed the \$5,000 threshold and have any red flags *must* be reported. The SAR-IC report must be filed within 30 days of the company’s detection of the suspicious activity. In instances that require immediate notice, the insurer can call the appropriate law enforcement agency and then file the SAR-IC.

The SAR-IC reporting requirement generally applies to transactions aggregating \$5,000 or more that the insurance company suspects

- involve funds derived from illegal activity
- are designed to evade federal reporting requirements
- have no apparent lawful purpose, or aren’t typical for type of customer making the transaction
- may be an attempt to use the insurance company in facilitating criminal activity.

Not all criminal activities involve laundered funds. The fourth category of reportable transactions—“attempt to use the insurance company in facilitating criminal activity” – exists to ensure the reporting of transactions involving legally derived funds that the insurance company suspects are being used for illegal purposes, such as terrorist financing.

Form 8300—Report of Cash Payments over \$10,000

While FinCEN’s rules require insurance companies to report suspicious transactions exceeding a \$5,000 threshold, companies are required to report *all* cash receipts exceeding \$10,000 without regard for red flags. First mandated by the Bank Secrecy Act of 1970 and made applicable to insurance companies by the USA PATRIOT Act, companies must file Form 8300, Report of Cash Payments Over \$10,000 Received in a Trade or Business within 15 days of receipt of either of the following:

- individual cash (or cash equivalent) payments exceeding \$10,000
- two or more related transactions totaling cash (or equivalent) payments exceeding \$10,000

Substantial penalties, equal to the greater of \$25,000 or the amount of reportable cash not reported, can be imposed on companies for noncompliance.

Confidentiality

FinCEN’s final rules prohibit an insurance company from disclosing the fact that it has filed a Suspicious Activity Report or disclosing information in that report to any other party except appropriate law enforcement and supervisory agencies. This prohibition includes the customer. Producers and employees should never discuss any aspect of a suspicious activity report, including the fact that one was filed, with the customer.

This provision does not prohibit insurance companies from obtaining customer information from their agents and brokers as needed to detect and report suspicious activity. Likewise, it does not prohibit insurance companies from discussing with their agents and brokers information pertaining to suspicious transactions with which they are involved. Lastly, it does not prohibit two or more insurance companies from sharing information or discussing among themselves suspicious transactions in which they are jointly involved. This cooperation might be needed, for example, to help determine which institution will file the Suspicious Activity Report in such a case.

Retention of Records

Insurance companies are required to maintain copies of SAR-ICs and the original or business record equivalent (such as scanned copies) of any supporting documentation for a minimum of five years from the date of filing.

In addition to Form SAR-IC, insurance companies are required to report cash (or cash equivalent) receipts exceeding \$10,000. Insurance companies use Form 8300 for this reporting.

SECTION REVIEW – QUESTION 10

[Section IX, Page 21)

A suspicious transaction combined with which of the following dollar amounts would required a company to file Form 8300, Report of Cash Payments?

- a. \$5,000
- b. \$10,000
- c. \$25,000
- d. \$50,000

SECTION REVIEW – QUESTION 11

[Section IX, Page 19)

Under FinCEN rules which of the following exceeds the suspicious activity review threshold?

- a. \$5,000
- b. \$7,500
- c. \$10,000
- d. \$25,000

X. AML BEST PRACTICES

The success of a company's AML program relies on the consistent application of compliance principles by producers and employees. Red flags are not always apparent, and the most effective way to catch even those that aren't is through consistent use of AML best practices. Each insurer will establish its own best practice compliance guidelines, reflective of their business profiles and covered products, but they are likely to include or be similar to the following:

Remain Alert

Effective compliance requires constant vigilance in all business dealings. Criminal elements continually look for new ways to use life insurance and annuity contracts for money laundering purposes. A vigilant producer will question anything that doesn't make sense. Be skeptical of unusual requests or circumstances, and insist on getting full answers to questions, especially those involving identities, funding sources, and purpose. Be especially wary of accepting cash or cash equivalents.

Know the Customer

Insist on knowing the applicant's full name and residential address, plus answers to all other identification questions asked by the company. Visually verify information by inspecting identification documents carefully.

Determine the Purpose

Determining a customer's purpose for buying an annuity or life insurance policy has always been important. Recording a customer's intent and purpose for a product purchase is an important aspect of suitability. Anti-money laundering efforts may require a deeper look at the reasons for buying a product, especially if other unusual aspects appear in the case. Examples of red flags regarding purpose include the following:

Cash value is more important than death benefits. Insurance costs and policy fees make life insurance less suitable for savings or investment purposes than other financial products. Be alert for customers who seem more interested in the policy's cash value or its loan or withdrawal options than its death benefit.

Customer requests an insurance product by name. Most consumers are not familiar with the different forms of life insurance. Probe for an answer if the customer asks for a high premium (high cash value) product and can give no clear reason for that request.

Customer requests a policy that appears to be inconsistent with his or her insurance needs. Customers have many reasons for owning life insurance, but an application should conform to the client's needs and profile. For example, would a single 30-year-old customer who has no consistent form of income need three \$250,000 10-pay life insurance policies?

Know the Funding Source

With insurance, a logical place to look for signs of money laundering is with the funds used in paying a product's premium. Red flags include the following:

The customer makes or requests a pre-payment of insurance premiums. With apparent disregard for potential modified endowment consequences, the customer sends a cash equivalent payment far exceeding the annual premium.

The transaction involves cross-border wire transfers. International wire transfers are always cause for closer examination, but a red flag is raised if the first premium paid with the application is wired from a bank account outside the U.S.

The policy's funding involves large fund flows through nonresident accounts with brokerage firms. Complex fund transfer arrangements between brokerage accounts could be a logical need for a complicated business case, or it could indicate money laundering.

Insurance premiums exceed the customer's apparent means. The size of the policy and the associated premiums should be in line with a customer's needs and resources. For instance, a 28-year-old worker who reported \$30,000 in income last year and yet applies for a \$1 million 10-pay life insurance policy with a \$50,000 initial deposit should raise a red flag.

Better Safe than Sorry

Best AML compliance practices should be driven by the watchwords “better safe than sorry.” Producers must promptly and willingly communicate *all* suspicions to their managers and field compliance principals, regardless of the depth of the suspicion. In accordance with its AML policy, the company will then determine whether to escalate the issue and whether any formal reporting is necessary. When in doubt, a producer should err on the side of caution and report the matter to his or her compliance officer.

The foundation of the life insurance industry is built on trust. Companies diligently guard their reputations with the public, as must individual producers. Any hint of a connection to money laundering—no matter how distant or remote—can irreparably harm one’s reputation and business. For the benefit of all—consumers, the insurance industry, and the larger economies in which the industry operates—producers have a responsibility to participate actively in their companies’ AML training programs and keep a watchful eye open for suspicious activity.

Geographical Location

In addition to those cited above, an important indicator of possible suspicious activity is *geographical location* of the parties involved in a transaction. This indicator includes the customer’s address as well as that of related parties (such as third-party owners) and financial institutions involved in funding the transactions.

Customers and related parties who are from high-risk countries are a red flag. Two common resources used by insurance companies in identifying high-risk countries are the following:

- **Office of Foreign Assets Control (OFAC)** This is a division of the U.S. Department of the Treasury, OFAC enforces U.S. economic and trade sanctions against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC compiles and updates the list of high-risk countries. It also maintains a list of known or suspected money launderers and other criminals, known as the *Specially Designated Nationals and Blocked Persons* list.
- **Financial Action Task Force (FATF)** This is an international body whose purpose is to develop and promote policies to combat money laundering. Its members include nations from around the world.

SECTION REVIEW – QUESTION 12

[Section X, Page 22-23)

Which of the following is NOT considered an AML Best Practice?

- a. Determine the Purpose
- b. Create customer categories
- c. Remain Alert
- d. Know the funding source

XI. Unauthorized Entities

Unauthorized entities engaging in insurance are a serious and growing problem in Florida for consumers and agents. Consumers are substantially harmed with these entities failing to pay claims and defrauding through deception. Agents are unwittingly (sometimes knowingly) representing these entities and placing clients and themselves at risk. Florida law is violated under the guise of these unauthorized entities claiming to be ERISA exempt or some type of association plan that claims to not be insurance or to be exempt from Florida regulation. All of this is simply not true! This is a problem in the state of Florida and other states.

The problem of unauthorized entities selling unauthorized products originated in the health insurance arena, although the problem now seems to be spreading into property-casualty arena as well. These unauthorized entities promised low health insurance premiums, a promise fueled by skyrocketing health insurance premiums with legitimate health insurance carriers. In the current market, low health insurance rates just do not exist. The public and certain agents, apparently, were ripe for the picking by these scam artists. Remember, these are scams and the intent is to collect as much premium as possible without having to pay claims, or very few claims.

Unsuspecting licensed insurance agents are also vulnerable to this type of scam because representatives of the unauthorized entity will contact the licensed agents and send them (or give them in person) printed marketing materials touting the unauthorized entity and their bogus products which, again, gives the impression of legitimacy and credibility.

Maybe the agent is asking too many questions of the representative – is just a little too inquisitive – about who they are, where they're located, how long they've been in business, etc. The agent may even question the legitimacy of the product. Some scam artists tell agents their products do not have to be authorized by the Department because it is an ERISA plan, or that the plan is part of a MEWA (multiple employer welfare arrangement) or it's to be sold to labor unions – all the while stating that under any of these previously-mention circumstances, the products do not have to be approved or authorized by the Department.

The representative of the unauthorized entity might say, “It doesn’t require approval, because this is an ERISA plan.” Or, “It doesn’t require approval because this is plan is part of a MEWA plan.” Or “This plan doesn’t require approval because it’s for labor unions.” None of this is correct! Any product which contains an insurance component is required, by law, to receive authorization of that component by the Department before it can be sold in Florida. Any legitimate company representative who approaches you about selling and representing their products should not mind the scrutiny you put them under by verifying their status with the Department.

626.902 Penalty for representing unauthorized insurer

(1) In addition to any other penalties provided in the insurance code:

(a) Any agent licensed in this state who in this state represents or aids an unauthorized insurer in violation of s. 626.901 commits a felony of the third degree, punishable as provided in s. 775.082 or s. 775.083.

(b) Any person other than an insurance agent licensed in this state who in this state represents or aids an unauthorized insurer in violation of s. 626.901 commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(2) In addition to the penalties provided for in subsection (1), such violator shall be liable, personally, jointly and severally with any other person or persons liable therefore, for payment of taxes payable on account of such insurance under s. 626.938.

Agents or any other persons are prohibited from representing or aiding an unauthorized insurer. If an agent or any other person represents an unauthorized insurer, they are subject to severe penalties, including possible civil and criminal action. Agents are subject to suspension or revocation of their licenses and/or monetary penalties for violation of the unauthorized insurer law. Agents can be held liable for claims and losses not paid by unauthorized insurers. Agents who represent or aid an unauthorized insurer commit a felony of the third degree.

Don’t be fooled by phony products that sound too good to be true! Investigate before you sell or buy these plans. Check to see if an entity or plan is an authorized insurer by calling the Department of Financial Services at 877-693-5236 or 850-413-3089.

SECTION REVIEW - QUESTION 13

(Ref: Section XI, Page 26)

Any agent licensed in this state who in this state represents or aids an unauthorized insurer in violation of s. 626.901 commits what level of violation?

- a. Felony of the 3rd degree
- b. Felony of the 1st degree
- c. Misdemeanor of the 2nd degree
- d. Misdemeanor of the 3rd degree

XII. Section Review Questions – Answer Key

1. C
2. B
3. A
4. D
5. A
6. C
7. B
8. C
9. C
10. B
11. A
12. B
13. A