

AML: Understanding the Rules for Insurance Producers and Employees

© 2015 by WebCE, Inc. All rights reserved. All content is copyrighted by WebCE, Inc., International Risk Management Institute, Inc. (IRMI), or is used under license. No content may be reproduced, retransmitted, distributed, sold, published, broadcast or circulated by anyone, including but not limited to individuals in the same company or organization, without express written permission. You are permitted to use this content only for your personal, noncommercial purposes. (Purchase of a prelicensing education course includes a license for one person to use the course for 60 days from the date of shipment or activation.) You may not distribute course materials to individuals who have not purchased the course unless WebCE, Inc. has given you written permission to do so. You may not make the course materials available to others over a computer network, intranet, Internet, or any other storage, transmittal, or retrieval system. Although we strive to ensure that the course content is accurate, you use it with the understanding that the authors and publishers are not engaged in giving legal, accounting, tax, financial, or other professional advice.



Introduction

USA Patriot Act – October 26, 2001

Purpose:

- Deter and punish terrorist acts in the U.S. and around the world

- Enhance law enforcement investigation tools

- Provide additional tools to prevent, detect, and prosecute international money laundering and the financing of terrorism

Money laundering was pushed to the center stage of national security

On October 26, 2001 – less than two months after the 9/11 terrorist attacks– Congress enacted the USA PATRIOT Act. Its main focus is to deter and punish terrorist acts in the United States and around the world. To meet this goal, it added a host of new law enforcement measures to detect and apprehend terrorists. Specifically, the Act revised certain existing laws in order to, quote, *“provide additional tools to prevent, detect, and prosecute international money laundering and the financing of terrorism.”*

Recognized by the PATRIOT Act as a significant contributor to funding terrorism and organized crime, money laundering was pushed to the center stage of national security.

Overview

All financial institutions must create and maintain **anti-money laundering (AML) programs**

Insurance companies were included under this requirement, but additional guidelines were necessary to define how insurers should comply

FinCEN published final AML rules for insurance companies on November 3, 2005 – they became effective May 2, 2006

- Today, every insurance company that sells certain types of life insurance and annuity contracts must have an active AML program

To expand the efforts to fight money laundering, the PATRIOT Act requires that all financial institutions create and maintain *anti-money laundering*, or AML , programs. From the beginning, this requirement included insurance companies, but because of the nature and complexity of insurance products, additional guidelines were necessary to define how insurance companies were to comply and how their AML programs were to be designed.

On November 3, 2005, the Financial Crimes Enforcement Network -- FinCEN , a division of the Treasury Department -- published long-awaited final AML rules aimed specifically at insurance companies. These rules would become applicable 180 days later, on May 2, 2006. Today, every insurance company that sells certain types of life insurance and annuity contracts must have an active AML program.

Course Objectives

Help producers and employees better understand the value and intent of their insurer's AML program and the role they play in its success

Explain the risk, methods, and consequences of money laundering in the insurance industry

Describe how government and the insurance industry have responded to the money laundering issue

Offer best practice ideas to give more meaning to a producer's AML responsibilities

The goal of this course is to help you -- insurance company producers and employees -- better understand the value and intent of your company's anti-money laundering program and appreciate the role you play in its success. The course explains the risk, the methods, and the consequences of money laundering in the insurance industry, and describes government and industry's responses to this issue. The course gives special attention to the role producers and employees play in their company's AML program, and offers best practice ideas to give more meaning to the producer's AML responsibilities.

Learning Objectives

Demonstrate an understanding of money laundering and the three phases of the money laundering process

Provide examples of how insurance products can be used for money laundering

Explain the elements of an insurer's anti-money laundering program and suspicious activity reporting requirements

Identify and describe suspicious activity red flags and transactions

Demonstrate an understanding of a producer's personal responsibilities with respect to a company's AML program

By the end of this course, you should be able to:

- Demonstrate an understanding of money laundering and the three phases of the money laundering process
- Provide examples of how insurance can be used for money laundering
- Explain the elements of an insurance company's anti-money laundering program and suspicious activity reporting requirements
- Identify and describe suspicious activity red flags and transactions, and
- Demonstrate an understanding of a producer's personal responsibilities with respect to a company's AML program



End of Section

You have reached the end of this course section. Please click the "Exit" button to return to the course's Table of Contents.

Part 1: AML Background and Basics

- What Is Money Laundering?
- What is Anti-Money Laundering?
- The Money Laundering Process
- Life Insurance Products and Money Laundering

To set the stage, we'll start with a discussion of the background and basics of anti-money laundering . . .

What Is Money Laundering?

Money laundering: the process of filtering and integrating illegally obtained money into the monetary system in a way that hides its illicit origins

- Schemes or activities that conceal the identity, source, and destination of illicitly obtained funds
- Common money launderers: drug traffickers, terrorists, embezzlers, and con artists
- Money launderers often rely on the unwitting participation of others



Most people understand implicitly that money laundering is illegal, but not everyone knows what “money laundering” means. In its simplest form, money laundering is the process of filtering and integrating illegally obtained money into the legal monetary system in a way that permanently hides its illicit origins. It involves some kind of scheme or activity – or often, a maze of transactions -- that aims to conceal the identity, source, and ultimate destination of illicitly obtained money.

The most common types of money launderers are drug traffickers, terrorists, embezzlers, and con artists. Most people who participate in money laundering are fully aware of the role they play in the process, but others may not be. Those others might include, for example, a well-meaning insurance producer who sells a life insurance policy under unusual circumstances without checking deeper.

What Is Anti-Money Laundering (AML)?



Anti-money laundering: union of laws, regulations, policies, programs, and procedures to fight the elements that would launder money

- Government
- Law enforcement
- Businesses – including insurance companies

9/11 brought attention to financed terrorism and how money laundering is used to fund illegal and terrorist activities

Opposing the criminals and terrorists who launder money are various *anti*-money laundering forces – laws, regulations, policies, programs, practices and procedures - representing government, law enforcement, and business. Brought to the money laundering fight through federal laws like the PATRIOT Act, these forces have become a critical part of our national security. And included in the AML “team” are insurance institutions and their representatives.

Federal agencies, like the Treasury Department and the FBI, have been investigating money laundering for decades. But the 9/11 terrorist attacks brought this country’s attention to *financed* terrorism, and how terrorists – and others – use money laundering to fund their activities.

The Money Laundering Process

No single way to launder money – it involves any financial transaction (or a series of transactions) that moves cash (or other assets) from one location or form to another to hide its origins and, ultimately, make it appear legitimate

Three stages:

1. Placement
2. Layering
3. Integration

There is no single way to launder money. In fact, one of the striking things about money laundering is the various ways it's carried out. The term "money laundering" refers to any financial transaction, or 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. For the criminal, there's usually a price to pay for this transformation: by the time an illicit dollar completes a laundering process it may be worth far less than its original value. But for a money launderer, that's a small price to pay, when the ultimate goal is to *hide the money's illicit origins*.

Money laundering generally involves three stages: placement, layering, and integration.

Stage 1: Placement

Placement – injecting illicit cash or assets into the legal financial system by some means, to obscure the start of an audit trail

Convert cash into cash equivalents

- Cashier's checks
- Money orders
- Bank drafts
- Traveler's checks
- Wire transfers

Structuring

Breaking up large cash sums into smaller amounts through multiple transactions. If done to avoid or evade reporting, it's illegal.

The first stage in the money laundering process is placement. Placement injects the illicit cash into the legal financial system. The goal at this initial stage is to obscure the start of an audit trail, which means avoiding financial accounts or products that record ownership. The cover-up is typically achieved by converting cash -- in a series of transactions -- into cash equivalents, such as cashier's checks, money orders, bank drafts, traveler's checks, or wire transfers.

Structuring is characteristic of the placement stage. Structuring is the practice of breaking up large cash amounts through multiple smaller transactions for the purpose of evading reporting or recordkeeping requirements. Cash is converted into cash equivalents in a series of small transactions. If done to avoid or evade reporting requirements, it's illegal.

Stage 2: Layering

Layering – using cash equivalents obtained in the placement stage to purchase other financial instruments

- Cash equivalents are used as premiums and deposits for more sophisticated financial products
- Provide liquidity
- Distribute or disburse funds in a way that appears legitimate

Note 📌
"Sophisticated financial products" can include cash value life insurance and annuities.

The next stage in the money laundering process is layering.

In the layering stage -- to further obscure the money trail from its illicit source -- the cash equivalents obtained in the placement stage are used to purchase other financial instruments. It's easy to understand the need for other instruments: simply exchanging cash for money orders and then depositing those money orders into a personal bank account does little to hide the link between the criminal and the crime. Instead, a money launderer uses the cash equivalents as premiums and deposits for more sophisticated financial products that

One - provide liquidity and

Two - more importantly, distribute or disburse funds in a way that appears fully legitimate.

For this purpose, "sophisticated financial products" can include cash value life insurance and annuity contracts.

Stage 3: Integration

Integration – the “cleansed” money is circulated back to the criminal as legitimate funds and can then be integrated into the financial system

Note

Apparent legal origins are now attached to the funds: the “dirty” money is now “clean.”

The final stage in the money laundering process is called integration. Here, the cleansed money is circulated back into the hands of the criminal and ultimately into the financial system.

It’s like laundry that has 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 around in public. For any questions as to its source, there is a legitimate answer.

Life Insurance Products and Money Laundering



How can life insurance products be used for money laundering?

- Underwriting requirements put the contract buyer and insured under a microscope
- Insurance products impose policy fees, insurance charges, and surrender penalties

So, how does all of this relate to insurance? Can life insurance products be used to launder money? At first thought, you might not think so. Underwriting requirements put the buyer and potential insured under a microscope, right? In addition, most life insurance products carry policy fees, insurance charges, and surrender penalties that can diminish the contract's value.

On further consideration, though, it's not difficult to understand how these products could, in fact, serve as ideal tools for "cleansing" illicit funds.

Life Insurance Products and Money Laundering

Cash value life insurance and annuity contracts provide access to funds through:

- Policy loans
- Partial withdrawals
- Full contract surrenders
- Free look surrenders

Note

The insurance company check gives the payment – and the funds – legitimacy. Funds can be sent or wired anywhere.

Insurance products offer access to the larger financial system. Cash value life insurance and deferred annuity contracts allow owners to access funds through policy loans, partial withdrawals, or outright surrenders. Free-look surrenders are especially appealing because they avoid surrender charges, but having to pay a surrender charge is not a serious deterrent to those looking to launder money. Such fees are deemed a reasonable business expense for the privilege of accessing contract values on demand.

Regardless of the form the distribution of funds takes, the common denominator is the *insurance company check* that gives the payment legitimacy. Funds derived in this manner appear fully legal and can be sent or wired anywhere.

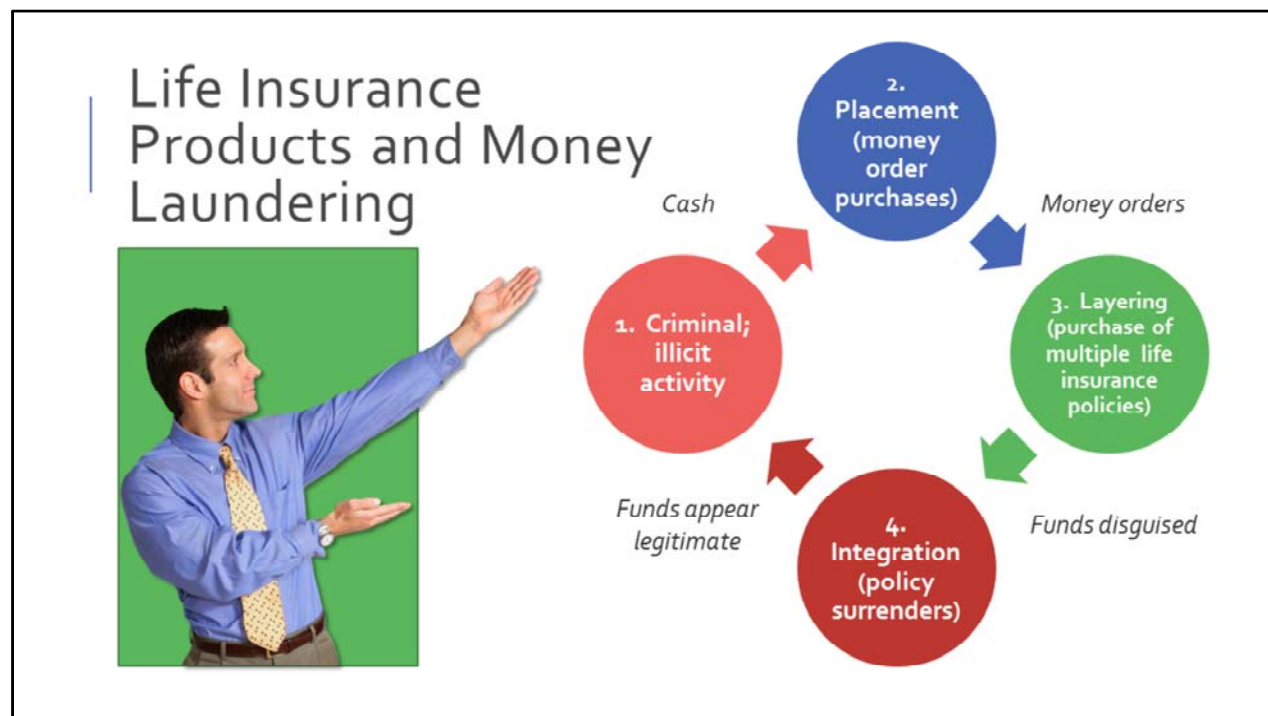
Life Insurance Products and Money Laundering

Aspects of the insurance business that could encourage money laundering:

- Financial institutions consider payments originating from insurance companies as common
- Insurance company payments do not attract attention
- Insurance products are diverse and easily available
- Substantial sums can be placed in insurance products
- Ownership can be easily transferred and assigned
- Products are widely available through brokers or other intermediaries who are not necessarily under the direct supervision of the company that issues the product

In addition, consider some the unique aspects of the insurance business itself that could encourage or promote money laundering:

- First, financial institutions consider payments that originate from insurance companies as commonplace; these payments don't attract attention.
- Insurance products are diverse and are easily available.
- Large amounts of money can be invested or placed in insurance products.
- Contract ownership can be easily transferred and assigned.
- Insurance products are widely available through brokers or other intermediaries who aren't necessarily under the direct control or supervision of the company that issues the product.



For example, here's a diagram of how a life insurance product could be used in the process of money laundering. One – you have large amounts of cash from criminal or illicit activity. Two – That cash is used to purchase a number of money orders from a number of different places – that's the placement stage. Three - The money orders are used to buy multiple life insurance policies, possibly over a period of time – that's the layering stage. Four - The life insurance policies are then surrendered and cashed out - that's integration.

The proceeds from these transactions – now in the form of the checks issued by the insurance company – now appear legitimate and can be integrated back into the hands of the criminal and the financial system.

Case Study: Operation Capstone

Colombian drug traffickers used life insurance companies in the U.S., Great Britain, and other countries to launder \$80 million of drug proceeds

These traffickers – through insurance brokers – bought high-premium, cash value life insurance policies with tens of millions of dollars of drug proceeds

Premiums were sent to insurers by third parties around the globe using cashier's checks and wire transfers

Here's a real-life example of how life insurance can be used to launder money.

In 2002, a sophisticated international money laundering operation was exposed in which life insurance companies in the United States, Great Britain, and other places around the world had been used to launder some \$80 million worth of Colombian drug proceeds over the previous three years.

Code-named Operation Capstone, the law enforcement action involved the coordinated efforts of the U.S. Customs Service, the U.S. Attorney for the Southern District of Florida, and several police departments in South Florida, as well as British and South American authorities. They discovered 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, using cashier's checks and wire transfers.

Case Study: Operation Capstone

Policyowners – associates of Colombian drug cartels -- were funding these policies just short of modified endowment policy (MEC) levels, and would make early withdrawals to access the policies' values; changes in policy ownership were common

Policyowners would receive checks or wire transfers from the insurance companies that appeared to be legitimate insurance proceeds

The laundered funds were then available to fund the drug cartels' interests

Operation Capstone revealed that the policyowners -- all associates of Colombian drug cartels -- were heavily funding their policies just shy of MEC levels 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 simply a cost of doing business.

The policyowners would receive checks or wire transfers from the insurance company that, on the surface, appeared to be legitimate insurance proceeds. The laundered money was now available to fund anything that served the cartels' interests.

Case Study: Operation Capstone

More than 250 insurance policies were found to be linked to drug proceeds

Overfunding life insurance policies and then making early withdrawals is an effective money laundering technique

Authorities realized that independent insurance brokers had little or no training in detecting money laundering

Conclusion: Insurance companies, like other financial institutions, are susceptible to money laundering; Congress was right to include insurance companies in the mandates set forth in the USA PATRIOT Act.

International Narcotics Control Strategy Report, Bureau of International Narcotics and Law Enforcement Affairs, March 2004

All told, authorities identified more than 250 insurance policies that were linked to drug proceeds. As reported in an International Narcotics Control Strategy report, over-funding life insurance policies beyond their face value, and then making early withdrawals – as these criminals did – is an effective money laundering technique. Operation Capstone also revealed that independent insurance brokers had little or no training in anti-money laundering issues, and were easily manipulated to place funds into nonbank financial institutions.

At the time – remember, this took place in 2002 -- anti-money laundering techniques and processes were not enforced in our industry. Insurance companies provided limited oversight over their many brokers and sub-brokers, and failed to recognize indicators of potential money laundering. Operation Capstone showed that insurance companies, like other financial institutions, are susceptible to money laundering. And it proved that Congress was right to include insurance companies in the AML mandates set forth in the PATRIOT Act.



End of Section

Money laundering has long existed as a means to integrate “dirty” funds into the economic system
Money laundering moves illicit funds through three stages: placement, layering and integration
The events of 9/11 elevated money laundering to a matter of national security, and prompted passage of the USA Patriot Act
All financial institutions – including covered insurance companies – must establish AML programs

This concludes Part 1 of the course. Here are some key take-aways:

- Money laundering has long existed as a way for illegal ventures to integrate “dirty” funds into the economic system without a trace of their illicit source. It’s a process that moves illegally obtained money through three stages: placement, layering, and integration.
- Law enforcement has tried to deter money laundering for decades. But the events of 9/11 elevated the issue to one of national security. To assist in the battle against terrorism, the USA PATRIOT Act of 2001 brings insurance companies into the fight.
- With its expenses, contract fees and surrender charges, life insurance would seem an unlikely object for money launderers. Real cases reveal otherwise. The PATRIOT Act requires insurance companies to establish anti-money laundering, or AML measures to prevent the use of their products in money laundering or terrorist activity financing, and to report “suspicious activities.” The cooperation of a company’s producers is essential to any such program’s success.

Part 2: Regulatory Basis for Anti-Money Laundering

Evolution of AML Laws
Bank Secrecy Act of 1970
USA PATRIOT Act of 2001
FinCEN Final AML Rules for Insurers

In this section of the course, Part 2, we'll address the regulatory basis for anti-money laundering and the two laws that most directly brought AML measures to the insurance industry. We'll then discuss the FinCEN requirements that pertain specifically to insurers, their producers, and their employees.

Evolution of AML Laws

Bank Secrecy Act -
1970



USA PATRIOT Act -
2001

Federal anti-money laundering laws have evolved dramatically over the past several decades. The modern era of AML regulations began in 1970 with the enactment of the Bank Secrecy Act. The law that most impacted insurance companies, the USA PATRIOT Act, descends directly from that law. Though there have been many AML laws in-between, these two are the most important to our study.

To fully understand today's AML requirements, let's review the Bank Secrecy Act – BSA.

Bank Secrecy Act of 1970 (BSA)

First significant federal AML law

Requires financial institutions to record and report information about customers' financial transactions

Enacted based on Congressional findings that such records and reports are useful for law enforcement, and tax, intelligence, and regulatory authorities

Note

"Financial institutions" include:

- Banks, credit unions, thrifts
- Broker/dealers
- Loan and finance companies
- Investment companies
- Travel agencies
- Casinos
- Insurance companies

The Bank Secrecy Act of 1970 – the BSA -- is generally regarded as the first significant federal AML law in the U.S. It established the requirement that financial institutions must record and report information about their customers' financial transactions, notably those that involve large amounts of cash. This requirement is based on earlier Congressional findings that such information is extremely useful for law enforcement and for tax, intelligence, and regulatory authorities. The title of this law is kind of misleading, since its intent is to *limit*, not promote, secrecy regarding financial transactions.

The BSA has been amended several times since its passage, with each amendment expanding its scope and reach. Today, BSA requirements extend to many different types of institutions: banks, credit unions, thrifts, broker/dealers, loan and finance companies, investment companies, travel agencies, casinos, and – significantly – insurance companies.

Bank Secrecy Act of 1970 (BSA)

BSA's notable requirements:

- Cash payments over \$10,000, received from one buyer for a single transaction, or for two or more related transactions, must be reported to the IRS (Form 8300)
- Businesses and individuals who own foreign bank accounts with total values exceeding \$10,000 must report the accounts 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"

Note

The fact that BSA regulations were found to be highly useful in the fight against financial crimes was reconfirmed with passage of the USA PATRIOT Act.

The Bank Secrecy Act involves many, many requirements. Among the most notable are these:

- Cash payments over \$10,000 that are received in a trade or business from one buyer for a single transaction or for two or more related transactions must be reported to the IRS. Form 8300 is used for this purpose. Note that insurance companies were brought into this requirement well before 2001.
- Businesses and individuals who own foreign bank accounts, brokerage accounts, mutual funds, unit trusts, or other financial accounts with aggregate value exceeding \$10,000 are required to report the account annually to the IRS.
- Banks must file a Suspicious Activity Report – a SAR for [quote] "any suspicious transaction relevant to a possible violation of law or regulation."

The BSA proved to be very useful in fighting financial crimes. This was reconfirmed in 2001 with passage of the USA PATRIOT Act.

The USA PATRIOT Act of 2001

Expanded the scope and purpose of the BSA to include “intelligence or counter-intelligence activities, including analysis, to protect against international terrorism”

Extended certain BSA requirements to non-bank financial institutions, including insurance companies and brokerage firms

Increased the ability of law enforcement agencies to search electronic communications, and medical and financial records

Expanded the Treasury Department’s authority to regulate financial transactions

In the days and weeks following the September 11, 2001, terrorist attacks, Congress worked to shore up the weaknesses in the U.S. economic system that may have contributed to the horrible events of that day. Less than two months after 9/11, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act—more simply, the USA PATRIOT Act. It was enacted on October 26, 2001.

Among its provisions, the PATRIOT Act amended the Bank Secrecy Act to extend BSA’s scope and purpose to include – quote - *“intelligence or counter-intelligence activities, including analysis, to protect against international terrorism.”* It also extended certain BSA requirements to nonbank financial institutions, including insurance companies and brokerage firms. In addition, the act increased the ability of law enforcement agencies to search electronic communications and medical, financial, and other records. Significantly for the insurance industry, it expanded the Treasury Department’s authority to regulate financial transactions, particularly those involving foreign individuals and entities.

The USA PATRIOT Act of 2001

Focus of PATRIOT Act: financial transactions that might be involved in terrorist financing

- Title III – Specifically addresses money laundering, and amended the BSA by:
 - Enhancing reporting obligations
 - Toughening standards for transaction “structuring”
 - Requiring the implementation of AML programs by all financial institutions, including life insurance companies
 - Recognizing that some insurance products can be – and are – used in money laundering schemes

The PATRIOT Act didn’t focus on money laundering *per se* but instead on any financial transaction that might be involved in terrorist financing. Particularly relevant to the insurance industry is Title III of the Act, which *does* specifically address money laundering. Title III amended the Bank Secrecy Act to:

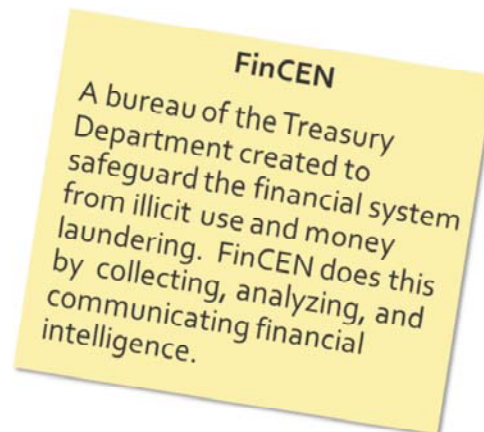
- Enhance reporting obligations
- Toughen standards for transaction structuring
- Require the implementation and oversight of anti-money laundering programs by all financial institutions, including life insurance companies.

Remember, the business of insurance is primarily regulated at the state level; the PATRIOT Act brought anti-money laundering requirements to the industry *nationwide*. The fact that the Act included insurance companies was an acknowledgment that some insurance products can – and are -- used in money laundering schemes.

FinCEN Final Rules for Insurers

The nature and complexity of insurance products raised questions about how insurers were to comply with the PATRIOT Act

On November 3, 2005, FinCEN issued final rules that address how insurance companies must comply with AML requirements



It was clear from the beginning that insurance companies were intended to be included in the PATRIOT Act's definition of "all financial institutions" and that they would be required to develop anti-money laundering programs. But the nature and complexity of insurance products raised many questions about how insurance carriers were to comply with these requirements – questions that took some time to work out. On November 3, 2005, the U.S. Treasury Department's Financial Crimes Enforcement Network – Fin-CEN -- published two long-awaited final rules geared specifically towards insurance carriers. FinCEN is a bureau of the Treasury Department, charged with administering the BSA.

FinCEN Final Rules for Insurers

1. Establish and maintain a risk-based AML program that
 - Reflects the unique money laundering risks the company faces
 - Prevents the company's "covered products" from being used for money laundering
2. Report "suspicious activity" involving covered product transactions by filing suspicious activity reports (SARs)

Note 📌
These FinCEN rules are at the heart of insurance company anti-money laundering programs.

First, insurance companies must *establish and maintain a risk-based anti-money laundering program*. "Risk-based" means that a company's AML program reflects the unique money laundering risks it faces. The intent is to prevent a company's "covered products" - mainly cash value life insurance and deferred annuity contracts -- from being used in money laundering or terrorist financing. The second set of FinCEN final rules adds insurance companies to the Bank Secrecy Act's list of those required to report "suspicious activity" involving covered product transactions. This is done through filing suspicious activity reports, or SARs . These two FinCEN rules are at the heart of insurance company anti-money laundering programs. We will discuss them in detail throughout the rest of the course.

Federal AML Bureaus and and Offices



And for those who want to understand a bit of the AML hierarchy of who does what at the federal level, here's a basic diagram. It shows a few of the offices and departments under the U.S. Department of Treasury that are charged with the fight against money laundering and financial crimes, here at home and internationally. As you can see, the Financial Crimes Enforcement Network – FinCEN – is only one of many. For the insurance industry, FinCEN provides outreach and training on implementing BSA compliance requirements, including AML programs and suspicious activity report filings. OFAC works with state regulators and the NAIC to detect and prevent money laundering schemes that involve violations of U.S. trade and economic sanctions.



End of Section

Two laws serve to bring insurance companies into the fight against money laundering: the Bank Secrecy Act and the USA PATRIOT Act

In 2005, FinCEN released final rules that explain how insurance companies are to comply with anti-money laundering requirements

In the main, the final rules require insurers to establish and maintain AML programs and to report suspicious activity by filing SARs with the federal government

You've now completed Part 2 of the course. Let's review some of the main points: There are two primary laws that serve to bring insurance companies into the fight against money laundering: the Bank Secrecy Act of 1970 and the USA PATRIOT Act of 2001. The PATRIOT Act's inclusion of insurance companies recognized the fact that some insurance products can be used in money laundering schemes. Due to the complexity of insurance products, it took some time before rules were released that explain how insurers are to comply with anti-money laundering requirements – this was accomplished by FinCEN in 2005. The final rules require certain insurers to establish and maintain AML programs, and to report suspicious activity by filing suspicious activity reports – SARs -- with the federal government.

Part 3: AML Rules for Insurance Companies

- Insurer Obligations Under the PATRIOT Act
- AML Compliance Program
- Covered Products
- Know the Customer (CIP)
- Agents and Brokers

In this section of the course, we'll discuss AML rules for insurance companies and the specific obligations they have under FinCEN and the PATRIOT Act, including establishing anti-money laundering programs. We'll also review covered products, "know your customer" programs, and the role of agents and brokers in supporting AML efforts.

Insurer AML Obligations Under the PATRIOT Act

Insurance companies that sell “covered products” must:

- Develop and maintain internal policies, procedures and controls to identify and report potential money laundering transactions
- Designate an AML compliance officer to oversee the company’s AML policies
- Develop and maintain an ongoing training program for all associates who are involved in the sale and administration of “covered products”
- Maintain an internal audit procedure to test the company’s AML policies and procedures

Note 📌
These elements must be defined and explained in a written document.

The PATRIOT Act’s mandate that all financial institutions establish AML programs is key to the national effort to prevent and detect money laundering and terrorism financing. It recognizes that other financial institutions – not just banks – are vulnerable to this threat. Therefore, as clarified by FinCEN’s final rulings, the PATRIOT Act stipulates that insurance companies involved in the sale of “covered products” have certain anti-money laundering obligations. They must:

- Develop and maintain internal policies, procedures and controls to identify and report potential money laundering transactions
- Designate an AML compliance officer to oversee the company’s AML policies
- Develop and maintain an ongoing training program for all associates who are involved in the sale and administration of “covered products,” and
- Maintain an internal audit procedure to test the company’s AML policies and procedures

These four requirements will constitute the core of a company’s AML program. They must be defined and explained in a written document, and made available to FinCEN. All four requirements seem clear enough, but what do they mean in practice? Let’s see . . .

AML Rules Apply to “Covered Products”

Covered products – those determined by FinCEN to present a higher risk for money laundering

- Individual permanent life insurance: whole life, universal life, variable life and any other product that builds cash value
- Individual annuities: fixed, indexed, or variable; immediate or deferred
- Any other insurance product that includes a cash value or investment component

Common characteristic:
Internal cash value that can provide liquidity.

First, it’s important to understand that the AML rules don’t apply to every insurance company or to every insurance product. They are aimed at companies that sell *covered products*. In this context, “covered products” are those that FinCEN determined as being at higher risk for money laundering.

Covered products include:

- Individual permanent life insurance - whole life, universal life, variable life and any other product that builds cash value
- Individual annuities - fixed, indexed or variable; immediate or deferred and
- Any other insurance product that includes a cash value or investment component. This ensures that any new life insurance or annuity product designs that include these characteristics would be covered.

What’s the common element that applies to these types of products? An internal cash value. Cash values can provide liquidity, or other ways to obtain cash, such as through policy withdrawals, loans, or as loan collateral.

Products That Are Not “Covered”

Term and credit life
Group life or group annuity products
Products offered by charitable organizations, such as charitable annuities
Property, casualty and liability insurance
Health insurance
Title insurance
Reinsurance and retrocession contracts
Contracts of indemnity and structured settlements (including workers compensation)

Note 📌
FinCEN determined these products do not present a high risk for money laundering.

Products that do *not* provide liquidity aren’t covered by the PATRIOT Act or FinCEN’s final rules – any product that does not include an internal cash value is not subject to AML requirements.

So, excluded from the definition of “covered products” are:

- Term, credit life and group life or group annuity products
- Products offered by charitable organizations, such as charitable annuities
- Property, casualty, and liability insurance
- Health insurance
- Title insurance and
- Reinsurance and retrocession contracts, and contracts of indemnity and structured settlements, including workers compensation

FinCEN determined that these products don’t represent a high risk for money laundering.

Insurers Subject to AML Requirements

Insurance companies that issue or underwrite covered products are subject to AML requirements

- Broker/dealers in securities are subject to independent AML program obligations
- If the insurance company is registered with the SEC as a broker/dealer, it does not have to establish a duplicate AML program as an insurance company
- The insurer should evaluate its AML program to ensure it addresses the risks of doing business in covered securities and insurance products

Note 📌
Non-covered products that an insurer issues do not have to be included in the company's AML program.

In the final FinCEN rule, the term “insurance company” or “insurer” is defined as any person or business engaged in issuing or underwriting “covered products.” If an insurance company that’s not issuing or underwriting a covered product should do so in the future, it would then become subject to the rule, to the extent of its business relating to covered products. Likewise, if an insurance company ceases issuing or underwriting covered products, it would no longer be subject to the rule. Broker/dealers have their own, independent AML obligations. An insurance company that’s registered with the Securities and Exchange Commission as a broker-dealer in securities would *not* be required to establish a duplicate program under the rule for insurance companies. However, it must evaluate to what extent its existing AML program addresses the risks of doing business in covered insurance products.

If, in addition to covered products an insurer issues *non*-covered products – property/casualty coverage, health insurance, or term life – the noncovered products don’t have to be included in the company’s AML program.

AML Compliance Program

Requirement: Designate a compliance officer

- Oversees the program's development, and assures it is effectively implemented and maintained
- Sees to the day-to-day operation of the company's AML program
- Ensures that the program's requirements are fully implemented and followed
- Thoroughly understands the money laundering or terrorist financing risks of the insurer's products and client base



Ok – so now you know what kinds of insurers and what kinds of insurance products come under the anti-money laundering requirements. Let's take a closer look at the steps insurers must follow to create a compliant AML program.

The first responsibility is to *designate an AML compliance officer* who's in charge of overseeing the program's development, and making sure it's effectively implemented and maintained. The compliance officer is responsible for the day-to-day operation of the company's AML program -- he or she makes sure that the requirements or steps laid out in the program are fully implemented and followed. The compliance officer should have a thorough understanding of the money laundering or terrorist financing risks of the insurer's products and client base.

AML Compliance Program

Requirement: Develop and incorporate internal policies, procedures and controls to help identify and report potential money laundering transactions

- The policies, procedures and internal controls are based on an internal risk assessment
- The program should reflect the money laundering risks that are associated with the company's covered products and business methods
- A thorough risk assessment is the basis for the company's AML program

The next step is to create an anti-money laundering policy and program. In the words of the law, an insurer's AML program must include "*internal policies, procedures and controls to help identify and report potential money laundering transactions.*" These policies, procedures and controls must be unique to each company, based on an internal *risk assessment* – that is, an assessment of the money laundering and terrorist financing risks that are associated with the company's covered products and its methods of operation. It's actually the risk assessment that forms the basis for how a company defines and develops its AML program.

AML Compliance Program



Risk-based evaluation of:

- Covered products contract provisions
- How products can be purchased
- Customer profiles and demographics
- Distribution channels
- Transaction processes
- International presence

Using a risk-based assessment gives companies latitude in designing an AML policy that fits their unique profiles. A company must evaluate the money laundering risks it faces that relate to:

- the company's covered products and the provisions in those products
- how the company's products can be purchased
- demographic profiles of their customers
- the company's distribution channels
- the company's transactions processes and
- the company's international presence

AML Compliance Program

Element:	Evaluate for possible risks posed by:
Covered products contract provisions	Early surrenders, withdrawals, policy loans
How products can be purchased	Cash vs. checks vs. money orders; initial vs. on-going premium payments
Customer profiles and demographics	Nonresident aliens, privately held corporations, charitable organizations
Distribution channels	Independent producers, international brokers
Transaction processes	How producers receive and transmit premiums and deposits
International presence	Countries identified as sponsors of terrorism

For example, for these elements of an insurer's business, here are some considerations that should be evaluated for the potential money laundering risk they might present.

- The company's covered products and the provisions in those products— what are the surrender, withdrawal and loan provisions and limits?
- How can the company's products be purchased—for example, cash versus checks versus money orders. Is there a difference between the kinds of premium payments allowed for initial product purchase versus on-going payments?
- Demographic profiles of the company's customers – these should be evaluated, especially those who are nonresident aliens, privately held corporations, small businesses, and charitable organizations
- Likewise, the company's distribution channels should be assessed, especially those involving independent producers and international brokers
- What about the company's transactions processes – are there any risks with how producers receive and transmit customer premiums and deposits to the company?
- And the company's international presence – does it issue or underwrite covered products in countries that have been identified as sponsors of international

terrorism?

Insurers should use their own expertise about their industry and their particular lines of business to develop their AML policies and procedures. An important element of this is a “customer identification program,” which we’ll get to shortly.

AML Compliance Program

Requirement: Develop and maintain an ongoing training program

- Producers and associates involved in the sale and administration of the company's covered products must be trained on the company's AML program
- Producers and associates represent the "front lines" in detecting suspicious activity and suspicious sales

Ok. Returning to the requirements of an insurer's AML program - the rules also mandate that insurers must develop and maintain an *ongoing training program* for producers and associates who are involved in selling and administering covered products. Insurers must integrate their agents, brokers and sales associates into their AML programs, and training plays a big part. Producers and sales associates – those who are on the front lines of the company's sales and product placement efforts – are absolutely key to helping a company identify and detect suspicious activity.

AML Compliance Program

Requirement: Maintain an independent audit procedure to test the adequacy of the company's AML program

- Frequency of testing depends on the company's risk assessment of its covered products
- Testing can be performed by an outside auditing or consulting firm, or by employees of the company – **not** the compliance officer
- Testing may involve the company's agents and brokers
- Recommendations resulting from testing must be submitted to senior management for consideration

The final element of an insurance company's AML program is *periodic testing* to ensure the program is working as it's intended to. The frequency of testing isn't mandated – it depends on the company's assessment of the risks associated with its covered products. As to who does the testing, it can be done by an independent auditing or consulting firm, or by a committee of the company's employees -- as long as the tester is *not* the compliance officer. Often, testing will consist of transactions that involve covered products – transactions that *should* trigger a red flag -- and will include the company's agents and brokers to see what happens. Results and recommendations from the testing must be submitted to the company's senior management for review.

As part of your overall responsibilities, you should be familiar with the required components of an insurance company's AML program. The next screen provides a review.

Know Your Customer

Customer Identification Program (CIP)

- Should be incorporated into an insurer's AML program
- Collect customer information that is necessary to detect suspicious activity and provide reasonable assurance that the customer's true identity is known
 - Legal name
 - Date of birth
 - Residential address
 - Social Security number or TIN
 - Driver's license or passport

As part of the AML program requirement to develop risk-based policies and procedures, insurance companies should have some kind of **customer identification program**, or C-I-P. Informally, this is referred to as “know your customer.” Though insurers are not *required* to create a formal C-I-P, the fact remains they have to gather all relevant and appropriate customer-related information that's necessary to run an effective anti-money laundering program.

Accordingly, in addition to the basic identifying customer information necessary for the insurer's everyday business practices, insurers should also obtain customer-related information that can help detect suspicious activity -- strange or unusual behavior and requests made by the customer -- and provide reasonable assurance that the customer's true identity is known. At a minimum, companies should identify the customer's:

- full legal name
- date of birth
- residential address, or address of next of kin
- Social Security number or tax identification number

Asking for a legal document, such as a driver's license or passport, should be part of the program – one that can be performed in the field by a producer.

Know Your Customer

Verify whether the applicant's name appears on any government-provided list of suspected or known terrorists

No U.S. business or citizen can transact business with individuals or entities on such lists

"Specially Designated Nationals and Blocked Persons List"

A list of individuals, groups, and companies known to be associated with terrorists or drug traffickers. Their assets are blocked and U.S. persons cannot do business with them.

Within a reasonable time after a new account is opened or a new customer purchases a policy, insurers must determine whether the applicant's name is on a list of known or suspected money launderers, terrorist organizations, and other criminals. This list is maintained by the Treasury Department's Office of Foreign Assets Control – O-FAC - called the Specially Designated Nationals and Blocked Persons list. No American business or citizen – including insurers, agents and brokers -- can do business with individuals or entities on this list.

Know Your Customer

"Notice to Customer"

- Must be given to applicants for covered products
- Informs applicants of the company's intent to verify their name and personal information
- Degree of verification effort is based on the extent of the risk
 - Amount of premium deposit
 - Unusual circumstances involving the transaction



As part of a C-I-P program, a Notice to Customer must be given to every applicant for a covered product. The purpose of the notice is to disclose the company's intent to verify the customer's name and personal information. The amount of effort required to verify the information will be based on the extent of the risk, such as the amount of premium deposit or unusual circumstances involving the transaction. Applicants who refuse to provide personal information will not be issued a policy or contract.

Agents and Brokers


Agents and brokers are not required to have separate AML programs,
but . . .

- As “front line” representatives, agents and brokers are vital in assisting their insurance companies with AML efforts, and are in the best position to:
 - Obtain customer information
 - Know the source of premium payments and other assets
 - Know the objectives for which the insurance products are purchased
- Insurers must integrate agents and brokers into their AML programs and monitor their compliance with the programs

So what about insurance agents and brokers? Are they – are *you* -- required to set up AML programs and procedures? No – you’re off the hook. Agents and brokers are not required to have separate anti-money laundering programs; the formal obligation rests with the insurer. *But*, because agents and brokers are so integral to the insurance business— after all, they’re the ones with direct contact with customers and direct involvement with sales -- they play a vital role in helping the insurance company in its anti-money laundering efforts. Agents and brokers are usually in the best position to:

- Obtain customer information
- Know the source of premium payments and other assets and
- Know the objectives for which the insurance products are purchased

For these reasons, insurers must integrate agents and brokers into their AML programs and monitor their compliance with the programs. Insurers are responsible for their AML program conduct and effectiveness, which includes the activities of their agents and brokers who are involved with covered products.



End of Section

Insurance companies involved in the sale of “covered products” must develop and maintain AML programs that meet four requirements

- Designate a compliance officer
- Maintain internal policies and controls to help identify and report potential money laundering transactions
- Maintain an ongoing training program for all associates who are involved in the sale and administration of covered products
- Periodically audit and test the program

We’ve reached the end of Part 3 of the course. Here’s a recap of some of the more important points we learned in this section.

The USA PATRIOT Act – as clarified by FinCEN final rules in 2005 -- mandates that financial services companies that sell or place “covered products” must comply AML requirements and design AML programs that meet four requirements:

- designate a compliance officer to oversee the company’s AML policies and procedures
- maintain internal policies, procedures, and controls to help identify and report potential money-laundering transactions
- maintain an ongoing training program for all associates involved in selling and administering covered products
- periodically test the company’s AML policies and procedures through an independent audit

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 and not their producers, producers’ front-line position puts them at the core of every company’s AML policy.

The next section of the course takes a closer look at the process by which insurance

companies review and report suspicious activity.

Part 4: SAR Rules and Requirements

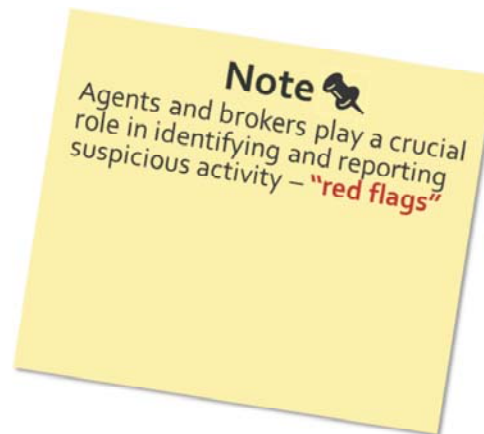
Suspicious Activity Reporting
SAR Reporting Guidelines
SAR Filing Procedures

Establishing a risk-based AML program – as we just discussed -- is one core requirement that insurance companies must meet to comply with federal anti-money laundering requirements. In this section of the course, we'll discuss the second major requirement: identifying and reporting suspicious activity.

Suspicious Activity Reporting

AML programs must include procedures to detect, review, and report **suspicious activity** and **suspicious transactions**

- **Law**—"Each insurance company shall file with FinCEN . . . a report of any suspicious transaction involving a covered product . . . relevant to a possible violation"
- **Goal**—To help federal government and law enforcement identify individuals, groups, and organizations involved in money laundering, terrorist financing, fraud, and other crimes, and to recognize emerging trends and patterns



An insurance company's AML compliance program is meaningless if the company doesn't have a process for detecting, reviewing, and reporting suspicious activity and suspicious transactions. Both the PATRIOT Act and FinCEN devote much attention to this aspect of anti-money laundering. Paraphrased, the law states, *"Each insurance company shall file with FinCEN a report of any suspicious transaction involving a covered product that is relevant to a possible violation of law or regulation."*

These reports provide detailed information about transactions that are or appear to be suspicious. The goal is to help the federal government and law enforcement identify individuals, groups, and organizations involved in money laundering, terrorist financing, fraud, and other crimes. FinCEN also uses the reports to identify emerging trends and patterns associated with financial crimes, which is critical to law enforcement.

Producers have a crucial role to play in the process of identifying and reporting signs of "suspicious activity"—what FinCEN calls red flags. We'll discuss red flags in a bit; first, let's review the what and why of suspicious activity reporting.

Suspicious Activity Reporting

FinCEN final rules require SAR reporting for insurance companies

- **What:**

- Transactions believed to involve funds from **illegal activity**
- Transactions believed to **disguise or hide funds** derived from illegal activity
- Transactions believed to be for **avoiding reporting requirements**
- Transactions believed to **use the insurer** to facilitate illegal activity

- **Why:**

- An insurer, its employees, and its agents are more likely than law enforcement to know when or if a financial transaction is suspicious

Requiring financial institutions to report suspicious financial transactions to federal authorities dates back to 1970 and the Bank Secrecy Act. Until the 9/11 terrorist attacks, insurance companies were generally exempt from suspicious activity reporting. But the PATRIOT Act and FinCEN's final rules changed that. Insurance companies are now required to identify and report suspicious transactions through the use of a Suspicious Activity Report, or SAR.

Specifically, the types of transactions to which SAR reporting applies are those that insurers have reason to believe:

- involve funds derived from illegal activity
- are meant to disguise or hide funds derived from illegal activity
- are done to avoid reporting requirements or
- are done to use the insurer to facilitate illegal activity

Requiring insurance companies – and other financial institutions – to report suspicious activity reflects a simple reality: the company and its employees and agents 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 in a better position to evaluate when a given purchase or transaction lacks legitimacy, in connection with the products or services the company provides.

SARs Are Risk-Based

The basis for monitoring and reporting suspicious activity should reflect the insurer's unique set of money laundering risks

- Covered products
- Distribution system
- Clientele
- Jurisdiction

Objective: Focus AML activities and resources where the money laundering risk is greatest

An effective anti-money laundering program uses a *risk-based* compliance process for identifying and reporting suspicious activity. As we've discussed, "risk-based" simply means that the company's AML program reflects its own unique set of money laundering risks: its covered products, its distribution system, its clientele, and its jurisdiction.

Risk-based reporting also traces back to the Bank Secrecy Act of 1970, which requires financial institutions to engage in risk-based compliance that focuses compliance resources where the money laundering risk is greatest.

SAR Reporting Guidelines

Key components for SAR monitoring and reporting

- Identify potential risks, based on company's risk assessment
- Map risks to red-flagged transactions and activity
- Monitor risk-based transactions and activity



Insurers should focus their anti-money laundering and suspicious activity efforts on monitoring risk-based scenarios, activity and transactions – mapping the company's money laundering risks to red-flagged transactions and activity. That should be the basis for SAR monitoring and reporting.

Transactions can be monitored manually by employees and compliance principals as part of the company's review escalation process. Or they can be monitored automatically using computer systems that identify transactions displaying red flag characteristics.

SAR Reporting Guidelines

Though money laundering transactions can involve any amount of money, most are of large sums

FinCEN suspicious activity review threshold:

- Any suspicious covered product transaction that includes a payment (or aggregate of payments) of **\$5,000 or more** must be investigated
- If suspicious activity is detected, the company must report the case to FinCEN
- Trigger transactions:
 - Policy withdrawals and loans
 - Cash value transfers and 1035 exchanges
 - Premium payments and deposits

Next, while transactions involving any amount of money may be used in a laundering scheme, the nature of the crime is such that it typically involves larger sums. Under FinCEN rules, the suspicious activity review threshold is \$5,000. Any suspicious covered product transaction that includes a payment --or aggregate payments --of \$5,000 or more requires the company to assess whether they need to file a SAR. Transactions that exceed 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.

Transactions that may trigger a review include policy withdrawals, loans, cash value transfers between policies and 1035 exchanges, as well as premium payments and deposits.

SAR Reporting Guidelines

Voluntary SAR reporting can be for amounts less than \$5,000

SAR monitoring and reporting can be for single transactions or patterns of transactions

SARs do not have to *prove* fraudulent or criminal activity

Note 📌
Form 8300: Insurers are required to report *all* cash receipts that exceed \$10,000, without regard to any red flags or suspicious activity

Insurers can *voluntarily* report transactions that appear relevant to violations of law or regulations, even in cases that fall below the \$5,000 threshold. Also, SAR monitoring and reporting aren't limited to single transactions – *patterns* of transactions are also subject to review. And it's important to understand that neither a company's SAR filing guidelines nor SAR reports themselves have to *prove* the actual existence of fraudulent or criminal activity – just the *suspicion*, based on facts and circumstances. SAR reports elevate the suspicion to another level – to FinCEN, or to law enforcement – who will take the appropriate next steps. It should be noted here that while FinCEN requires insurance companies to report suspicious transactions at or over a \$5,000 threshold, companies are required to report *all* cash receipts that exceed \$10,000, without regard for red flags or suspicious activity. This is done by completing IRS Form 8300 -- "Report of Cash Payments Over \$10,000 Received in a Trade or Business." Form 8300 must be filed within 15 days of receiving either a single or related payments over \$10,000. Of course, money launderers know about this \$10,000 threshold and will typically keep their transactions below this amount in order to avoid reporting requirements.

SAR Filing Procedures

What to file: Form SAR, along with supporting documentation

Where to file: With FinCEN

When to file: No later than 30 calendar days after the date of the initial detection of the suspicious activity

If no suspect is identified at initial detection, filing can be delayed for another 30 days

Note

In situations that require immediate attention – terrorist financing or ongoing money laundering schemes – the insurer must immediately notify a law enforcement authority.

So how are SARs filed?

An insurer reports suspicious transactions by completing what is known as Form S-A-R, and including supporting documentation and narration – a description of the event or activity or transaction, and why it raised suspicion. Form SAR is available and can be filled in online, and then e-filed with FinCEN.

A SAR should be filed within 30 calendar days after the date the insurance company first detects the activity or first becomes aware of facts or circumstances that support a SAR filing. If no suspect is identified on the date of initial detection, the insurer can delay filing a SAR for another 30 calendar days to identify a suspect. But in no case can reporting be delayed more than 60 calendar days after the date of initial detection.

In situations that require immediate attention, such as suspected terrorist financing or ongoing money laundering schemes, the insurance company must immediately notify FinCEN or an appropriate law enforcement authority, in addition to filing a SAR.

How SARs Are Used

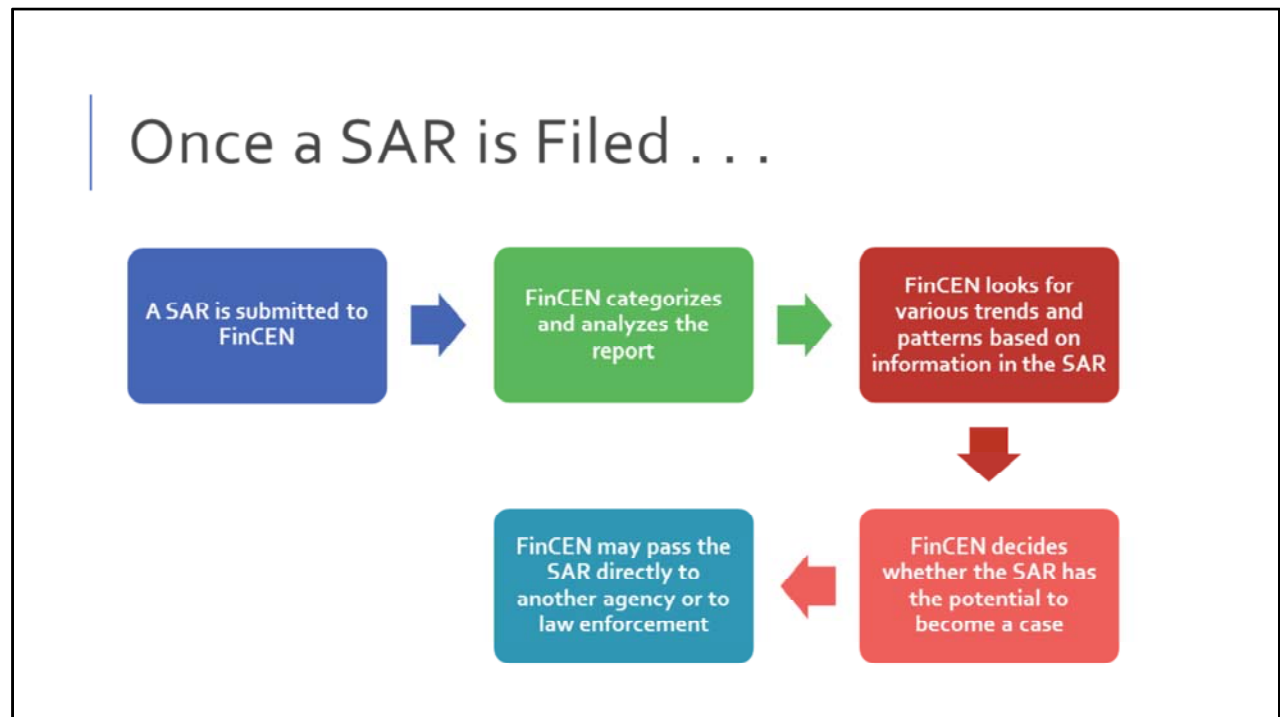
Law enforcement—To initiate and support investigations into money laundering, terrorist financing and other criminal investigations

Analysts—To identify trends and patterns associated with financial crimes and money laundering

Federal regulatory authorities—To review the compliance systems and procedures of financial institutions

How are SARs used? The reports are filed by insurance companies and other financial institutions to report suspicious activity, so what happens with this information? It's collected by FinCEN and used by a range of authorities:

- Law enforcement uses the information to initiate and support investigations into money laundering, terrorist financing and other criminal investigations
- Analysts use the information to identify trends and patterns
- Federal regulatory authorities, such as BSA and AML compliance personnel, use the information to ensure that institutions' AML programs and procedures are sound.



This diagram shows the basic path a SAR takes after it's been submitted to FinCEN. The agency categorizes and analyzes the report based on the standard information provided, as well as the narrative that describes the suspicious activity. When analyzing the report, it will look for various trends and patterns based on the information provided, and will decide whether the report has the potential to become an actual case. It may decide to cross-check the subject of the report with other financial reports and other data bases. It might decide to pass the report directly to another federal agency or to law enforcement. Obviously, at this point, the report is out of the insurer's hands, but it's testimony that the company contributed in a significant way to helping protect our financial system. The next screen details the elements of SAR report.

What Prompts a SAR Filing?

No hard or fast rules, only FinCEN guidelines

1. The transaction or activity involves a covered product
2. The transaction or activity involves at least \$5,000 in funds or assets
3. Facts or circumstances about the transaction or activity raise suspicion



So when is a suspicious activity report filed? There are no hard and fast rules; there's no black or white. In fact, SAR reports are typically surrounded by "gray." FinCEN's filing guidelines are:

1. The transaction or activity involves a covered product
2. The transaction or activity involves at least \$5,000 in funds or assets
3. Facts or circumstances about the transaction or activity raise suspicion

What Prompts a SAR Filing?

"A determination as to whether a 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.**"

FinCEN

Note

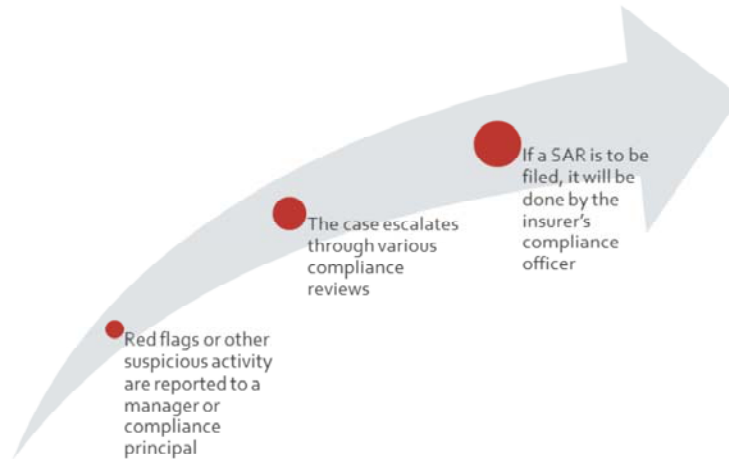
Insurers are **not** required to report submission of false or fraudulent information for purposes of obtaining a policy or making a claim, unless the information relates to money laundering or terrorist financing.

On that last point about what might raise suspicion, the rules state, "A determination as to whether a 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." A red flag is *any* fact or circumstance that is not typical for a customer, 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. We'll discuss red flags in the final section of the course.

Note that for AML purposes, insurers are *not* required to report the submission of false or fraudulent information by customers to obtain a policy or to make a claim, unless the information relates to money laundering or terrorist financing.

Who Files a SAR?



It's the responsibility of the insurance company and the company's compliance officer to file SARs and report suspicious activity to federal authorities. Producers do not. 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 – ever -- 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.

SARs Are Confidential

Insurers cannot disclose that a report has been filed or reveal anything about the report

- The subject of the report cannot be informed that a report has been filed
- Producers and employees must not discuss any aspect of a SAR with the customer

Confidentiality requirements do **not** prohibit insurers from:

- Obtaining customer information from producers or discussing suspicious activity that involved a producer
- Sharing information with other insurance companies on cases in which they are jointly involved

Unless it's to appropriate law enforcement or to federal or state agencies, insurers can't disclose anything about a suspicious activity report, including the fact that one has been filed. For example, a SAR filing can't be disclosed to a credit reporting agency. Nor can the subject of the report be told that a report has been filed. Producers and employees can't discuss any aspect of a SAR with the customer. This provision doesn't prohibit insurance companies from obtaining customer information from their agents and brokers as needed to detect and report suspicious activity. Likewise, it doesn't prohibit insurance companies from discussing with their agents and brokers information pertaining to suspicious transactions that involve their cases or clients. And lastly, it doesn't prohibit two or more insurance companies from sharing information or discussing among themselves suspicious transactions they are jointly involved in. This cooperation might be needed, for example, to determine which company will file the SAR.

SARs Are Confidential



Copies of SARs and any supporting documentation must be kept for a minimum of 5 years .

Copies of SARs and any supporting documentation must be kept for at least five years. Obviously, these reports must be kept securely.


SAR Safe Harbor

Insurers cannot be held liable for filing a SAR

"Any financial institution that makes a ... disclosure of any possible violation of law or regulation ... shall not be liable to any person under any law or regulation of the United States... for such disclosure or for any failure to provide notice of such disclosure to [any] person who is the subjectof such disclosure."

31 USC § 5318(g)(3)

Federal laws are intended to provide the greatest possible protection to financial institutions to encourage the filing of Suspicious Activity Reports if appropriate. For this reason, the law includes a "safe harbor." Specifically, the law states, "Any financial institution that makes a disclosure of any possible violation of law or regulation to a government agency shall not be liable to any person under any law or regulation of the United States for such disclosure or for any failure to provide notice of such disclosure to any person who is the subject of such disclosure or any other person identified in the disclosure."



End of Section

Insurance AML programs are risk-based and must include procedures to monitor, detect and report suspicious activity
Suspicious activity that involves covered products and amounts of \$5,000 or more must be reported to FinCEN, by filing a SAR
SARs are filed by a company's compliance officer; however, producers are responsible for reporting any suspicious activity to their manager or a designated compliance member
SARs are confidential; insurers cannot disclose that a report has been filed or reveal anything about the report, except to a federal or state agency, or to law enforcement

We've now reached the end of Part 4 of the course. Here are some of the more important points covered in this section:

- Insurance company anti-money laundering programs are risk-based, and must include policies and procedures designed to monitor, detect and report suspicious activity.
- Any suspicious activity that involves covered products and amounts of \$5,000 or more must be reported to FinCEN, by filing a suspicious activity report, or SAR.
- SARs are filed by a company's compliance officer; however, producers and employees are responsible for reporting any suspicious activity or red flags to a manager or a designated compliance member.
- SAR reports are confidential. Neither the insurer nor any of its associates can disclose anything about the report, including whether one has been filed. The exception is that disclosure can be made to an appropriate federal or state agency, or law enforcement.

Part 5: AML Red Flags

- AML Relies on Full Compliance
- AML Responsibilities for Producers
- Detecting Red Flags
- AML Best Practices

In this final section of the course, we'll discuss an aspect of anti-money laundering that directly involves producers and employees: helping identify red flags and detecting red flag activity. We'll also look at AML best practices that producers can incorporate into their day-to-day business practices.

AML Relies on Full Compliance

An insurer's AML program depends on its employees and producers:

- They must be aware of the realities of money laundering
- They must know their AML program and its requirements
- They must be committed to compliant AML business practices

An insurer's AML program very much depends on its producers and employees. Even though the PATRIOT Act and FinCEN rules don't impose AML compliance program requirements *directly* on agents and brokers, it's clear that federal authorities contemplated active involvement by producers and staff members when they designed AML requirements for insurance companies. Companies rely on their employees and producers to be aware of the realities of money laundering, to know their AML programs, and to comply with AML business practices.

AML Responsibilities for Producers

Obtain and verify an applicant's personal information

- Pursue answers to questions, especially those dealing with the customer's identity
- Ensure customers comply fully with the information requests of the insurer's CIP requirements
- Visually examine applicants' identifying documents

Monitor transactions and report suspicious activity

- Observe customers and their transactions for suspicious facts and circumstances not revealed in application questions
- Collect and retain information necessary to assess risks associated with high-risk businesses, geographic locations, or products that may be more susceptible to abuse

Producers are especially important to an insurer's AML efforts. As we've mentioned, they stand on the front lines, and often represent the only point of contact between the consumer and the insurer.

The producer's role in supporting anti-money efforts comes into play at many points. For instance:

Obtaining and verifying an applicant's personal information—Proper compliance means pursuing the answers to questions until the producer is satisfied that they are complete, especially those questions dealing with the customer's identity. It means knowing the customer and making sure the customer complies fully with the information requests of the company's customer identification program. It includes visually examining the applicant's driver's license or other identifying documents that the insurer has specified for this purpose.

Monitoring transactions and reporting suspicious activity—Producers are a company's eyes and ears in the field, giving them a key role in observing customers for suspicious facts and circumstances that might not be captured in application questions. Understanding that a company's AML program is risk-based, producers should expect to collect and retain information needed to assess risks associated with high-risk businesses or high-risk geographic locations, or those using products

that may be more susceptible to money laundering.

AML Responsibilities for Producers

Assist in AML investigations

- Producers who worked a case that is elevated to an AML investigation may be called on to provide additional information
- Discussion notes in the customer's file may provide important details

Participate in AML program testing

- Effective testing should start at the beginning of a typical transaction process – with the producer
- Adopt sound AML compliance practices and use those practices with every customer

Assisting in any AML investigation —If suspicious activity is detected, the company's AML Compliance Committee or compliance officer will commence an investigation to determine whether a SAR should be filed with the appropriate law enforcement or regulatory agencies. Producers and employees who may have worked on the case can expect to be called upon to provide additional information. Maintaining good discussion notes in the customer's file will help provide important details that might be missed if left to memory alone.

Participating in AML program testing—As directed by the PATRIOT Act, insurance companies are required to periodically test their AML programs through the use of independent auditors. To be most effective, the test needs to start at the beginning of the typical transaction process, with the producer. An agent or broker can do little to prepare for an AML audit. Producers are advised to adopt sound AML compliance practices as directed by their insurers and use those practices with every customer.

Detecting Red Flags

Red flag—Any fact, circumstance or customer request that is unusual or suspicious

- Request for a partial surrender from a recently purchased life policy - ???
- Request for a withdrawal with proceeds payable to an unrelated third party - ???
- Request for a transfer of ownership to an unrelated third party - ???

Any of these requests can be legitimate . . . or not

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. A red flag 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 there's a request that the withdrawal check be payable to an apparently unrelated third party. Or what about a request for a transfer of ownership of a newly issued policy to an apparently unrelated third party? Certainly, any of these requests could be legitimate . . . or not.

Detecting Red Flags

Producers are uniquely positioned to detect red flags

- Be alert for circumstances that don't make sense
- Ask follow-up questions to verify customer responses that seem unclear, unusual, or unexpected
- Be prepared to decline applications from individuals who will not or cannot comply with requests for identifying information
- Be alert to vague or evasive responses to questions about the intended use of the product
- Record notes of all conversations and observations
- Report all red flags as directed by the company's AML program

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 will observe, may raise a red flag hinting at suspicious activity. 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 customer answers that seem unclear, unusual, or unexpected, and 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. In these cases, the producer should accept the application but bring the matter to the attention of his or her manager or compliance principal
- record notes of all conversations and observations and
- report all red flags to their managers or field compliance principals as directed by the company's AML process. Remember: concerns or suspicions are *not* to be discussed with the customer nor should the producer contact federal authorities directly.

Red Flag Categories

As a general rule, red flags can be separated into four transaction categories:

- New business
- Premium and deposit payments
- Policy activity
- Geographic location of parties involved in an insurance transaction

FinCEN cites a number of red flag examples in its 2005 final rules, though the list is not all-inclusive. As FinCEN notes, “The techniques of money laundering are continually evolving and there is no way to provide an exhaustive list of suspicious transactions.” As a general rule, however, red flags can be separated into four transaction categories:

- new business
- premium and deposit payments
- policy activity and
- The geographical location of the parties involved in an insurance transaction

Let’s take a look at red flags that are associated with each of these categories.

New Business Red Flags

The source of the purchase premium is inconsistent with customer's financial profile

The applicant exhibits unusual concern with government reporting requirements, especially those involving personal identification information

The applicant wants to engage in a transaction that lacks business sense, or is inconsistent with a stated business strategy

The applicant appears to be acting as an agent for an undisclosed party

The applicant provides inconsistent answers or misleading information

The applicant (or associate) has a questionable background

First, there's new business: new customers, new accounts, new cases. This is where a lot of red flagged activity takes place. Red flags to watch for during transactions involving the sale and issue of *new business* include:

- The source of the funds used to purchase the product is inconsistent with the customer's financial situation or profile.
- The applicant exhibits unusual concern with government reporting requirements, especially those requiring personal identification information.
- The 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.
- The applicant appears to be acting as an agent for an undisclosed party or principal but is reluctant or refuses to provide information about that party.
- The applicant provides inconsistent answers to questions or misleading information.
- The applicant (or a person associated with the applicant) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

New Business Red Flags

The applicant lives in a distant local, though a comparable policy could be purchased where he/she lives

The applicant shows little concern about the performance of the product, but much concern about its withdrawal and surrender provisions

The applicant exhibits indifference for policy fees and charges

The applicant is rated, but unconcerned about higher premiums

The applicant is reluctant to provide identifying information

The applicant exercises the free-look return privilege shortly after policy issue

More new business red flags:

- The applicant lives in a distant locale, though a comparable policy could be purchased where he or she lives.
- The customer shows little or no concern for the performance of an insurance product but much concern about its withdrawals and surrender provisions.
- The applicant exhibits indifference for policy fees and charges, especially early surrender charges.
- The applicant is rated and shows casual disregard for the higher premiums he or she will pay due to the rating.
- The customer is reluctant to provide identifying information when purchasing an insurance product, or the customer provides minimal or seemingly fictitious information.
- The customer exercises the “free-look” privilege shortly after the policy is issued.

Also important to a new business case is understanding the *purpose* for which a policy or contract is being purchased. The next screen identifies some red flags you should be aware of when determining the reason for or purpose of the purchase.

Premium and Deposit Payment Red Flags

Any unusual method of payment, particularly by cash or cash equivalents

Payments received from unrelated third parties

Payments that are made through wire transfers in large amounts

Purchase of the product with monetary instruments in structured amounts ("structured settlements")

Purchase of the product with numerous checks drawn on different accounts

Large payments that are closely followed by requests for partial surrenders or policy loans

Moving on, red flags associated with *premium and deposit payments* include:

- any unusual method of payment, particularly by cash or cash equivalents
- payments received from unrelated third parties
- payments that are made through wire transfers of sizable amounts
- the purchase of an insurance product with monetary instruments in structured amounts ("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

Early termination of a product, especially at a cost to the customer or where refund check is directed to an unrelated third party

Lack of concern about surrender charges

Transfer of ownership to an apparently unrelated third party

Borrowing the maximum amount soon after policy purchase

A pattern of recurring policy loans with prompt repayments

Payment of unscheduled premiums, followed by policy withdrawals

Any request that a transaction be processed in a way that avoids normal documentation or normal procedures.

Now let's consider policy activity. Many policy transactions, such as a change in policy dividend options or the addition of a new beneficiary, are a normal part of insurance transactions and insurance business. But some aren't. Red flag *policy activities* are any that are unusual or atypical. For example:

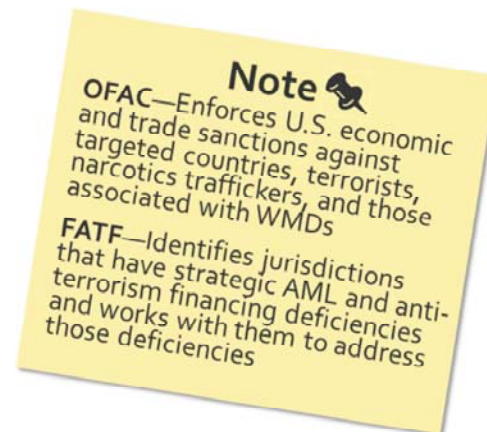
- the early termination of an insurance product, especially at a cost to the customer or where cash was tendered and/or the refund check is directed to an apparently unrelated third party;
- lack of policyowner concern or questions about surrender charges when requesting a policy surrender;
- the transfer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

Geographic Location Red Flags

Customers and related parties from high-risk countries

Resources used by insurers to identify high-risk countries:

- OFAC - *Specially Designated Nationals and Blocked Persons* list
- FATF – international body that develops and promotes policies to combat money laundering and terrorism financing



In addition to those we just discussed, an important indicator of possible suspicious activity is the *geographic 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 financial institutions in identifying high-risk countries are the Office of Foreign Assets Control, or O-FAC, and the financial Action Task Force, or FATF.

The Office of Foreign Assets Control (OFAC)—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.

The Financial Action Task Force (FATF)—FATF is an international body whose purpose is to develop and promote policies to combat money laundering. Its members include nations from around the world.

Producer and Employee Red Flags

Suspicious activity can be internal – demonstrated by a producer or employee

- Change in a producer's sales activity
- Change in an employee's behavior
- Issue must be escalated to the company's compliance officer

Not all red flags arise from the customer's side of the transaction. Some are raised by suspicious activity demonstrated by the producer or a company employee. Usually these red flags relate to a change in the producer's sales activity or employee's behavior. The change may be observed by the producer's or employee's manager, a field compliance principal, or a compliance officer. However detected, the matter is escalated 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 next screen includes a number of hypothetical scenarios that illustrate producer or employee activity that suggests a need for a closer review.

If You Encounter a Red Flag. . .

Report any red flag immediately

- Ideal: Create a written report summarizing:
 - Date of occurrence
 - Name, address, and other identifying information of the person(s) involved
 - Nature of the red flag that raised suspicion

Do not:

- Try to investigate
- Try to prove money laundering
- Discuss the situation with the customer

So, what should you do if you encounter a red flag?

First, report it immediately. Insurance companies are responsible for reporting suspicious transactions and suspicious activity that is conducted through its agents and brokers. Though you should follow the procedures set forth by your insurers, chances are they would require that any suspicious activity be reported through a written document. Ideally, the document would include:

- The date of the occurrence
- The name, address, and other identifying information of the person or persons involved and
- What was said or done that raised suspicion.

Now, what should you *not* do if you encounter a red flag? Do not try to investigate the matter. Do not try to prove money laundering. And do not discuss the situation with the customer. Leave any and all of the follow-up to the compliance officer.

AML Best Practices

Remain alert

- Effective compliance requires constant vigilance in all business dealings

Know your customer

- Insist on having all identification information asked by the company

Avoid “willful blindness”

- Exercise due diligence in all dealings with customers

Practice “better safe than sorry”

- When in doubt, err on the side of caution and report the matter to the compliance officer

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
- Know the customer - Insist on having all identification information asked by the company
- Avoid “willful blindness” - Exercise due diligence in all dealings with customers; keep your eyes open to the source of policy funds
- Practice “better safe than sorry” - When in doubt, err on the side of caution and report the matter to the compliance officer

A Final Thought . . .

Foundation of the life insurance industry is built on trust

- All those associated with the industry must guard this trust – and their reputations – with the public
- Any hint of a connection to money laundering can harm your reputation and business
- For the benefit of all, you have an important responsibility to actively participate in your company's AML program and be on the alert for suspicious activity



The foundation of the life insurance industry is built on trust. Companies diligently guard this trust – and 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.



End of Section

An insurer's AML program depends on active participation by producers, notably in helping to detect red flags and red flag activity

Red flags typically fall into four transaction categories: new business, premium and deposit payments, policy activity, and geographical location

Producers are in a unique position to help identify red flags in each of these categories, and should report any suspicious activity immediately

The keystones to AML best practices for producers: remain alert, know your customer, avoid willful blindness, practice "better safe than sorry"

This concludes Part 5 of the course. To review:

An insurer's AML program very much depends in on its producers and employees, especially with helping to detect red flags and red flag activity. Though it's impossible to provide a list of all suspicious transactions or activity, as a general rule, red flags can be associated with four transaction categories:

- new business
- premium and deposit payments
- policy activity, and
- The geographical location of the parties involved in an insurance transaction

Due to the role they play in the business, producers are in a unique position to identify red flags in each of these categories. Any red flags or any suspicious activity should be reported immediately to a compliance officer, including those that are observed internally. But because red flags aren't always apparent, anti-money laundering best practices dictate that producers should integrate certain principles into their day-to-day business activity:

- Remain alert
- Know your customer
- Avoid "willful blindness" and exercise due diligence in all dealings with customers and

- Practice “better safe than sorry.” When in doubt, err on the side of caution and report any suspicious activity to your compliance officer.