Anti-Money Laundering

Table of Contents

SECTION 1 OVERVIEW OF MONEY LAUNDERING

The purpose of this course is to help insurance professionals better understand the landscape of money laundering in the United States and to support the planning of efforts to combat money laundering.

Gauging the Problem

Criminals are taking advantage of globalization by transferring funds quickly across international borders. Technology developments allow money to move anywhere in the world with the speed of light. The United States are an economic powerhouse, serving as a beacon to the world. The crooked trail of money laundering often starts, passes through, or ends up here. The deeper 'dirty money' gets into the banking system, the more difficult it is to identify its origin. Money laundering is a clandestine affair making it difficult to estimate. Because of the clandestine nature of money-laundering, it is difficult to estimate the total amount of money that goes through the laundry cycle. The estimated amount of money laundered globally in one year is 2 - 5% of global GDP, or $800 billion - $2 trillion in US dollars. The margin between these figures is huge, but even the lower estimate underlines the seriousness of the problem.

Process

Money laundering is the processing of the proceeds of crime to disguise their illegal origin. Once these proceeds are successfully 'laundered' the criminal is able to enjoy these monies without revealing their original source. Money laundering can take place in various ways. Money laundering is often described as occurring in three stages: placement, layering, and integration.

1. **Placement:** refers to the initial point of entry for funds derived from criminal activities. The placement stage represents the initial entry of the funds into the financial system. For the drug trafficker, in particular, this is not necessarily an easy task. The immense cash profits of the illegal drug trade can pose an enormous problem. Cash is awkward to deal with regularly and in bulk: $200,000 in $10 bills weighs 40 lbs. Banknotes are also easily lost, stolen or destroyed.
2. **Layering:** refers to the creation of transactions which attempt to obscure the link between the initial entry point and the end of the laundering cycle. This is the most complex stage of the process, and the most international in nature. The money launderer might begin by sending funds electronically from one country to another, then break them up into investments in advanced financial options or in overseas markets, moving them constantly to evade detection, each time hoping to exploit loopholes or discrepancies in legislation and delays in judicial or police cooperation
3. **Integration:** refers to the return of funds to the legitimate economy for later extraction. In this final stage of money laundering the funds return fully assimilated into the legal economy. Having been placed initially as cash and layered through a number of financial operations, the criminal proceeds are fully integrated into the financial system and can be used for any purpose

The National Anti-Money Laundering Strategy

Money laundering is a necessary consequence of almost all profit-generating crimes and can occur almost anywhere in the world. It is difficult to estimate with any accuracy how much money is laundered in the United States. However, while recognizing the limitations of the data sets utilized, in 2015 the U.S. Treasury estimated that about $300 billion is generated annually in illicit proceeds. Fraud and drug trafficking offenses generate most of those proceeds.

The fight against money laundering and terrorist financing is an ongoing campaign that forms a critical part of national security. This theme is echoed throughout the several money laundering strategies promulgated over the years by the Treasury and Justice Departments.

Details of their strategy reflect the federal government's plan to deal with money laundering. The U.S. government has an ongoing commitment to attack money laundering and terrorist financing on all fronts, including the formal and informal components of both the domestic and international financial systems. Armed with tools provided by the USA PATRIOT Act, authorities are taking coordinated and aggressive action using all available means, including law enforcement actions, appropriate financial regulation and oversight, and coordination with private sector and international partners. While significant progress continues to be made, much remains to be done to confront the ever-changing, global threat of money laundering and terrorist financing.

Government policy represents a continuation of past efforts, and a commitment to move forward by identifying, disrupting, and dismantling high value terrorist financing and money laundering organizations and networks. The central tenet of the strategy is the ever-increasing need for all relevant U.S. government agencies, foreign government counterparts, and partners in the private sector to pool collective expertise and coordinate activities to stop the laundering of criminal proceeds and to staunch the flow of funds to terrorists. By attacking the financial infrastructure of complex criminal organizations and terrorist networks, long-term damage is inflicted on their ability to perpetuate criminal operations.

To achieve these objectives, a focus is placed on three major goals:
(1) to cut off access to the international financial system by money launderers and terrorist financiers more effectively;
(2) to enhance the Federal government's ability to target major money laundering organizations and systems; and
(3) strengthen and refine the anti-money laundering regulatory regime for all financial institutions to improve the effectiveness of compliance and enforcement efforts.

The National Anti-Money Laundering Strategy includes, among other items, a commitment to accomplish the following:

- Block and seize terrorist assets and identify and designate terrorist organizations.
- Target countries and institutions that facilitate money laundering and terrorist financing, including using the full range of measures provided by Section 311 of the USA PATRIOT Act.
- Take law enforcement action against high value money laundering targets, including those with ties to major narcotics trafficking operations.

- Improve the effectiveness of compliance and enforcement efforts to continue to strengthen and refine the anti-money laundering regulatory regime for all financial institutions by identifying new and emerging threats that can be addressed through regulation, improving the effectiveness of anti-money laundering controls through greater communication, guidance, and information-sharing with the private sector, and enhancing regulatory compliance and enforcement efforts.
- Encourage foreign countries throughout the world to adopt and adhere to international standards to inhibit the flow of illicit funds, both through the formal and informal financial sectors, and to assist in developing and enhancing anti-money laundering regimes in targeted countries to enable them to thwart terrorist financing.
- Improve the Federal government's partnership with the private financial sector to increase information-sharing and close the gaps in the financial system that allow abuse by money launderers and terrorist financiers.

The National Anti-Money Laundering Strategy both targets terrorist financing as a top priority and directs improvement of our ongoing efforts to combat money laundering. It embodies our conviction, deepened by our growing experience in this area, that the broad fight against money laundering is integral to the war against terrorism.

At the same time, the plan embraces anti-money laundering efforts as key to attacking all kinds of other criminal activity, including narcotics trafficking, white collar crime, organized crime, and public corruption. Resources devoted to fighting money laundering and financial crimes reap benefits far beyond addressing the financial crimes they directly target. Financial investigations expose the infrastructure of criminal organizations; provide a roadmap to those who facilitate the criminal activity, such as broker-dealers, bankers, lawyers and accountants; lead to the recovery and forfeiture of illegally-obtained assets; and support broad deterrence against a wide range of criminal activity. Thus, the National Anti-Money Laundering Strategy is intended to sharpen ongoing efforts to combat money laundering by ensuring that law enforcement agencies and task forces use and share all available financial databases and analytical tools, focusing law enforcement personnel and other resources on high-impact targets and financial systems, and improving Federal government interaction with the financial community.

Although money laundering and terrorist financing differ in certain ways, they share many of the same methods to hide and move proceeds. Moreover, both depend on a lack of transparency and vigilance in the financial system. Accordingly, our efforts to identify and target shared-methods to place, layer, and transfer money -- such as by using the informal financial sector, including alternative remittance systems; bulk currency shipments; money transmitters; money changers; and commodity-based trade--will help us combat both those who launder criminal proceeds and those who finance terrorism.

Briefly, money laundering depends on the existence of an underlying crime, while terrorist financing does not. Methods for raising funds to support terrorist activities may be legal or illegal, and the transactions tend to be smaller and much less observable than, for example, the typical narcotics money laundering transaction. Moreover, money laundering investigations are initiated to achieve prosecution and forfeiture. Terrorist financing investigations share these objectives; however, their ultimate aim is to identify, disrupt and cut off the flow of funds to terrorists, whether or not the investigation results in prosecutions.

Who is required to comply?

It's important to note that not all insurance companies are required to comply with the Financial Crimes Enforcement Network (FinCEN) ruling. In keeping with the scope of the PATRIOT Act, the final rule focuses on those covered insurance products possessing features that make them susceptible to being used for money laundering or the financing of terrorism. "Covered Products" include
(1) a permanent life insurance policy, other than a group life insurance policy;
(2) any annuity contract, other than a group annuity contract; and
(3) any other insurance product with features of cash value or investment.

To the extent that the risk for abuse is lower, term life insurance, group life, group annuities, and insurance products offered by property-casualty insurers or by title or health insurers are not, at this time, included in the definition of "covered products." In addition, those insurers required to meet the new regulations must have an AML program that meets the following criteria:
1. The program must be in writing.
2. The program must be approved by senior management.
3. The program must be made available to FinCEN upon request.

In addition, the AML program must:
1. Be tailored to meet each company's assessment of the money laundering and terrorist financing risks of its products.
2. Designate a compliance officer responsible for ensuring that the program is implemented effectively and is updated as necessary.
3. Provide for ongoing training of appropriate personnel.
4. Provide for independent testing to ensure adequacy.

Suspicious Activity Reporting (SARs)

As with banks and broker dealers before them, insurance companies subject to the regulations will also have to have processes in place to file Suspicious Activity Reports or SARs with the authorities. Such reports have in the past been controversial within the financial industry as regulators have often found banks filing SARs for reasons that are often outside of what would be considered "suspicious" activity. Banks and other institutions have contended that it is better to be "safe than sorry" and without clear direction from regulators of what constitutes suspicious behavior have erred on the side of caution. Here is the FinCEN view, summing up what many regulators believe has been excessive SAR filing:

> "While the volume of filings alone may not reveal a problem, it fuels our concern that financial institutions are becoming increasingly convinced that the key to avoiding regulatory and criminal scrutiny under the Bank Secrecy Act is to file more reports, regardless of whether the conduct or transaction identified is suspicious. These 'defensive filings' populate our database with reports that have little value, degrade the valuable reports in the database and implicate privacy concerns."
> (FinCEN SAR Review)

In contrast the Center for Regulatory Compliance with the American Bankers Association offers the view of bankers and others in the financial industry:

> "Until the financial sector receives assistance in the form of guidance and clear examples of what constitute suspicious activity, the volume of suspicious activity reports (SARs) will continue to skyrocket."

While insurance companies might initially adopt the same risk-averse approach in terms of SAR filings, there are clear differences between the insurance sector and other parts of the financial industry, and some industry bodies have provided concrete examples and guidance as to what to watch out for when examining customer behavior and transactions. The limited definition of insurance company for purposes of the rule, as well as the final rule requiring insurance companies to file SAR's, is not intended to limit the kinds of financial institutions that may voluntarily report suspicious activity under the protection of the safe harbor from liability contained in 31 U.S.C. 5318(g)(3).

Agent Responsibilities under Money Laundering Rules

Insurance producers are an important part to play in insurance companies' anti-money laundering programs. Agents and brokers have direct contact with the insurance-buying public. This puts them in the best position to be the "eyes and ears" of any effort to gather information and detect suspicious activity. It is true that the new regulations do not require insurance producers to establish anti-money laundering programs themselves, but are required to integrate agents and brokers into programs. This will help ensure that insurers and their sales force personnel work together in the prevention of money laundering. Some method of monitoring compliance must also be a part of the program. If the incorporation of agents into the anti-money laundering programs of insurance companies nationwide is deemed unsuccessful by FinCEN, it has the option to reconsider the decision not to require agents and brokers to establish their own programs.

Insurance companies are required to maintain a written anti-money laundering program applicable to "covered products." The program must be reasonably designed to prevent the insurance company from being used to facilitate money laundering or the financing of terrorist activities. Companies must also report suspicious activities and establish guidelines to make it possible to obtain information from producers to detect and report such transactions.

Risk-based compliance: Each institution is different

Similar to the banking and securities industry insurance providers will need to adopt a risk-based approach to meet the new AML requirements. What does this mean? No two institutions are identical in terms of the way they conduct business, whether in terms of their client base, geographical reach, sales and distribution channels or products offered. Therefore, each company will have its own unique profile which should allow for a determination of which parts of the business are more at risk than others.

Developing such a risk-based approach is one that regulators have repeatedly stressed to the financial industry – in other words: "You know your business better than we do." As such, the decision on what type of AML solution is appropriate will first require a risk

assessment of the company’s numerous businesses and potential risks or hot spots. The assessment process should include at least the following:

• Risk identification/categorization of customers, beneficiaries, products, and business locations.
• Assessment of AML infrastructure, including compliance program development and implementation.
• Benchmarking to peers, other financial services sectors, and AML compliance legal and regulatory standards, including the USA PATRIOT Act, the BSA, and international guidance.

BSA Overview

In 1970 Congress passed the Currency and Foreign Transactions Reporting Act, otherwise known as the "Bank Secrecy Act" (BSA) that established requirements for recordkeeping and reporting by banks and other financial institutions. The BSA was designed to help identify the source, volume, and movement of currency and other monetary instruments into or out of the United States or U.S. financial institutions. The statute sought to achieve that objective by requiring individuals, banks, and other financial institutions to create a paper trail by keeping records and filing reports determined to have a "high degree of usefulness in criminal, tax and regulatory investigations and proceedings." Part of the paper trail was the filing of Currency Transaction Reports, or CTRs, for currency transactions in excess of $10,000. CTRs and other reports enable law enforcement and regulatory agencies to pursue investigations of criminal, tax and regulatory violations. More recently, in response to the 9/11 terror attacks, Congress passed the PATRIOT Act, more formally known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. Title III of the Patriot Act is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.

Anti-Money Laundering Programs

Under the Bank Secrecy Act, all financial institutions must develop, administer, and maintain a program that ensures compliance with the BSA and its implementing regulations, including reporting and recordkeeping requirements, and each federal banking agency, including the Federal Reserve, has specific rules requiring such programs. Anti-money laundering compliance programs should be tailored to a financial institution’s business operations and risks, and if followed by company personnel, should ensure full compliance with all legal requirements, as well as effective risk management.

Customer Identification Program

Under the BSA, as amended by the Patriot Act, every financial institution must implement a written Customer Identification Program (CIP) appropriate for its size, location, and type of business. The CIP must be incorporated into the institution's anti-money laundering compliance program and must be approved by the institution's board of directors. The CIP must include account-opening procedures that specify the identifying information that will be obtained from each customer, and it must include reasonable and practical risk-based procedures for verifying the customer's identity. These procedures must enable the institution to form a reasonable belief that it knows the true identity of each customer.

Suspicious Activity Reporting Requirements and Customer Due Diligence
Under the Bank Secrecy Act and the suspicious activity reporting rules promulgated by the Federal Reserve, the other federal banking agencies, and Treasury in 1995, banking organizations are required to report to the government any instances of known or suspected criminal or suspicious activity by filing a Suspicious Activity Report, or SAR. To ensure that it will be able to identify suspicious activity, a banking organization should have in place a customer due diligence (CDD) program under which the organization (1) assesses the risks associated with a customer account or transaction, and (2) gathers sufficient information to evaluate whether a particular transaction warrants the filing of a SAR. In addition, appropriate systems, processes, and controls should be in place to monitor and identify suspicious or unusual activity. Common processes include employee referrals, manual systems, automated systems, or any combination, which vary based on the risk and size of the banking organization (See Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29,398 (May 11, 2016)).

Know your customer

Know Your Customer (or 'KYC') is the due diligence obligation that financial institutions perform to identify their clients and ascertain relevant information pertinent to doing financial business with them. Typically, KYC is a policy implemented to conform to a customer identification program mandated under the Bank Secrecy Act and USA PATRIOT Act. Know your customer policies have becoming increasingly important globally to prevent identity theft fraud, money laundering and terrorist financing. In a simple form these rules may equate to answering a series of questions, but this is the tip of the iceberg and regulators now expect much more. KYC should not be thought of as a format to be filled - it is a process to be undergone from the start of a customer relationship to the end.

One aspect of KYC checking is to verify that the customer is not on any list of known fraudsters, terrorists or money launderers, such as the Office of Foreign Assets Control's Specially Designated Nationals list. This list contains thousands of entries that are updated at least monthly. As well as sanctions lists there are lists of third party vendors that track links between persons regarded as high-risk owing to negative reports in the media about them or in public records. Beyond name matching, a key aspect of KYC controls is to monitor transactions of a customer against their recorded profile, history on the customer’s account(s) and with peers.

SECTION 2 BANK, TRUST & MONEY SERVICES

Banks and other depository financial institutions in the United States are unique in that they alone are allowed to engage in the business of receiving deposits and providing direct access to those deposits through the payments system. The payments system encompasses paper checks and various electronic payment networks facilitating credit and debit cards and bank-to-bank transfers. The unique role banks play makes them the first line of defense against money laundering.

Banks- Financial Backbone

Depository financial institutions (DFIs), which include commercial banks, savings and loan associations (also called thrifts), and credit unions form the financial backbone of the United States. The term “bank” will be used generically in this chapter to refer to all forms of DFI. Although Money Service Businesses (MSBs) may offer an alternative to banks, MSBs must themselves engage the services of a DFI to hold deposits, clear checks, and settle transactions. Thus in almost every money laundering typology, a bank is employed domestically or abroad to hold or move funds. The stage at which funds are introduced into the banking system is a critical one. “Once a person is able to inject funds into the payment system that are a product of a criminal act or are intended to finance a criminal act, it is highly difficult, and in many cases impossible, to identify those funds as they move from bank to bank.”[1] The BSA requires banks to establish and maintain effective anti-money laundering (AML) programs, implement customer identification programs, and maintain transaction records. Banks also are obligated to report cash transactions exceeding $10,000 as well as transactions that appear suspicious.

Going Paperless

A significant development in the banking sector is the ongoing decline in the use of paper checks. In 2000, checks were used in more than 40 billion transactions, according to a recent report from the Federal Reserve’s Cash Products Office. That number is down to less than 20 billion, according to the Fed’s most recent numbers, which are based on a survey conducted in October 2012. For banks and retailers, the very distinction between checks and electronic forms of payment has become blurry. Checks are now regularly scanned for MICR information and converted into automated clearinghouse transactions.

Face-to-Internet

The shift from paper to electronic payments is changing the economics of the payments business, putting emphasis on lowering costs. In response, banks are increasingly using the Internet as a means for customers to open or access accounts. Moving away from face-to-face customer interaction, particularly for account openings, challenges the traditional process of customer due diligence. Similarly, the steady influx of immigrants without U.S. Government-issued identification is requiring banks to explore new ways to verify the identity of their customers.

Vulnerabilities

Banks, although obligated to implement a customer identification program, must contend with businesses and consumers who may attempt to disguise their true identity and source of income. Cash-intensive businesses, for example, may inflate how much legitimate cash comes in each day to disguise the deposit of cash from illegal drug sales or other criminal activity. Banks attempt to spot these deceptions at the point accounts are opened or to recognize suspicious deposit and withdrawal activity as it occurs.

---

[1]Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking, sponsored by the New York Clearing House Association, LLC, March 2002

As banks venture into opening accounts online and providing online account access, it becomes increasingly difficult to verify customer identification. The move away from face-to-face account opening and account access creates opportunities for fraud and identity theft. Unauthorized access to checking accounts is the fastest growing form of identity theft. In October 2005, the Federal Financial Institutions Examination Council (FFIEC), a body composed of the DFI federal regulatory agencies, issued industry guidance titled: Authentication in an Internet Banking Environment. The document advises financial institutions offering Internet-based products and services to use customer authentication techniques "appropriate to those products and services." In addition to the difficulty financial institutions face identifying their customers online, the growing adoption of electronic payment systems is producing new opportunities for electronic fraud.

Table 1 SAR Filings

Illustrated below is the total volume of SAR filings over several years.

FinCEN Suspicious Activity Report (FinCEN Form 111)
Filings by Year & Month by an Insurance Company
March 1, 2012 through December 31, 2016

Month	2012	2013	2014	2015	2016
January	0	219	211	159	176
February	0	211	265	174	204
March	0	189	273	180	231
April	11	320	290	183	213
May	13	262	277	192	205
June	17	318	232	177	181
July	89	280	231	209	180
August	60	307	223	207	171
September	41	196	206	184	197
October	155	236	172	196	194
November	158	261	155	209	218
December	182	267	200	235	219
Subtotal	**726**	**3,066**	**2,735**	**2,305**	**2,389**
Total Filings	**11,221**				

*Statistics generated for this report were based on the Bank Secrecy Act Identification Number of each record within the Suspicious Activity Report system. The Bank Secrecy Act Identification Number is a unique number assigned to each Suspicious Activity Report submitted. Numeric discrepancies between the total number of filings and the combined number of filings of states and/or territories are a result of multiple locations listed on one or more Suspicious Activity Reports.

Note: Statistical data for Suspicious Activity Reports are continuously updated as information is processed. For this reason, there may be minor discrepancies between the statistical figures contained in the various portions of this report.

Source: FinCEN SAR Stats Technical Bulletin March 2017

Trusts

Legal jurisdictions, whether states within the United States or entities elsewhere, that offer strict secrecy laws, lax regulatory and supervisory regimes, and corporate registries that safeguard anonymity are obvious targets for money launderers. The use of bearer shares, nominee shareholders, and nominee directors function to mask ownership in a corporate entity. While these mechanisms were devised to serve legitimate purposes, they can also be used by money launderers to evade scrutiny.

Trusts separate legal ownership from beneficial ownership and are useful when assets are given to minors or individuals who are incapacitated. The trust creator, or settlor, transfers legal ownership of the assets to a trustee, which can be an individual or a corporation. The trustee fiduciary manages the assets on behalf of the beneficiary based on the terms of the trust deed.

Although trusts have many legitimate applications, they can also be misused for illicit purposes. Trusts enjoy a greater degree of privacy and autonomy than other corporate vehicles, as virtually all jurisdictions recognizing trusts do not require registration or central registries and there are few authorities charged with overseeing trusts. In most jurisdictions, no disclosure of the identity of the beneficiary or the settlor is made to authorities. Accordingly, trusts can conceal the identity of the beneficial owner of assets and, as will be discussed below, can be abused for money laundering purposes, particularly in the layering and integration stages.

Regulation and Public Policy

Trust companies are defined as “financial institutions” under the Bank Secrecy Act. Shell companies are not specifically listed in the BSA, but could be regulated under the BSA under one of the two catch-all provisions of 31 USC 5312(a), given an appropriate record.

Money Services Businesses

Money Services Businesses (MSBs) provide a full range of financial products and services outside of the banking system. For individuals who may not have ready access to the formal banking sector, MSBs provide a valuable service. They also pose a considerable threat. MSBs in the United States are expanding at a rapid rate, often operate without supervision, and transact business with overseas counterparts that are largely unregulated. Moreover, their services are available without the necessity of opening an account. As other financial institutions come under greater scrutiny in their implementation of and compliance with BSA requirements, MSBs have become increasingly attractive to financial criminals.

MSBs Defined

Under existing BSA regulations, MSBs are defined to include five distinct types of financial services providers (including the U.S. Postal Service (USPS)):

(1) currency dealers or exchangers;
(2) check cashers;
(3) issuers of traveler’s checks, money orders, or stored value cards;
(4) sellers or redeemers of traveler’s checks, money orders, or stored value; and
(5) money transmitters.

The list indicates and reality shows there is great variance in characteristics and vulnerabilities across the various types of MSB's.

Vulnerabilities

The fleeting nature of the customer's relationship with an MSB is a significant vulnerability. In contrast to banks, one does not need to be an existing "customer" of an MSB and a customer can repeatedly use different MSBs to transact business. This makes customer due diligence very difficult. MSBs are used at all stages of the money laundering process. More than one violation may be identified on a single SAR. These reports point most commonly to customers attempting to evade the $3,000 funds transfer recordkeeping requirement (or the $3,000 recordkeeping requirement for cash purchases of money orders or traveler's checks) by either breaking up a large transaction into smaller transactions or by spreading transactions out over two or more customers.

Many people still prefer to use MSBs for financial services because of convenience, cost, familiarity, or tradition. More than a quarter of American households use non-bank financial institutions such as MSBs, to do everything from paying their bills and cashing checks to supporting their family members abroad. An MSB is defined by regulation (31 C.F.R. § 1010.100(ff)) to be any person, wherever located, doing business wholly or substantially in the United States, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities:

- Money transmitter
- Check casher
- Issuer or seller of money orders
- Issuer or seller of traveler's checks
- Dealer in foreign exchange
- Provider or seller of prepaid access

All principal MSBs, except for the United States Postal Service, are required to register with FinCEN and to establish a written AML program reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities (31 C.F.R. §1022.210 and §1022.380). Additionally, the BSA requires MSBs to file CTRs and SARs and maintain certain records. The MSB recordkeeping requirements ($3,000 for money orders and traveler's checks) are specific to purchases of cashier's checks, money orders and traveler's checks, dealers in foreign exchange and money transmitters (31 C.F.R. § 1010.415, § 1022.410 and § 1010.410(e)–(f)). In addition, many states have licensing criteria for certain types of MSBs such as money transmitters and check cashers. There were 41,788 MSBs registered with FinCEN as of April 2015.

Historically, consumers have chosen to send remittances abroad largely through money transmitters such as Western Union and MoneyGram. The federal recordkeeping requirement for money transmitters, and certain other MSBs, allows funds transfers below $3,000 without requiring the verification and recording of the customer's identification or sending certain information about the transmitter and the transaction with the payment. Individuals in the United States send approximately $37 billion annually to households abroad. The average remittance from the United States to Latin America was estimated in 2011 to be only $290 while the average to Mexico was $400.

Section 359 of the USA PATRIOT Act expanded the definition of financial institution to include any person who engages as a business in an informal value transfer system (IVTS) or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside the United States.

Virtual Currency

Virtual currency is not legal tender but can be transferred from entity to entity, person to person, as a substitute for legal tender and later converted into real currency. In July 2011 FinCEN published a final rule amending, among other things, the definition of money transmitter, adding the language “or other value,” so the definition now reads: “the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." (31 C.F.R. § 1010.100(ff)(5)(i)(A))

FinCEN provided guidance clarifying that based on certain activities that constitute money transmission, administrators and exchangers of convertible virtual currency are money transmitters, and are required to comply with the same registration, AML program, recordkeeping, and CTR and SAR reporting obligations that apply to money transmitters. An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency (Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN- 2013-G001).

In 2015, San Francisco-based Ripple Labs Inc., the developer and seller of a virtual currency known as XRP, was cited by FinCEN in the first civil enforcement action against a virtual currency exchanger. FinCEN cited Ripple Labs and a wholly-owned subsidiary with willfully operating as an MSB and selling its virtual currency without registering with FinCEN, failing to implement and maintain an adequate AML program, and failing to report suspicious activity related to several financial transactions. Concurrent with FinCEN’s enforcement action, DOJ reached a settlement agreement with Ripple Labs to resolve a criminal investigation into the Bank Secrecy Act violations. FinCEN assessed a $700,000 civil money penalty concurrent with the U.S. Attorney's Office for the Northern District of California's settlement agreement, which included a forfeiture of $450,000.. The $450,000 forfeiture in the DOJ settlement was credited to partially satisfy FinCEN’s $700,000 civil money penalty (http://www.fincen.gov/news_room/nr/pdf/20150505.pdf).

Centralized virtual currencies have a centralized repository and a single administrator. Liberty Reserve, which FinCEN identified in 2014 as being of primary money laundering concern pursuant to Section 311 of the USA PATRIOT Act, is an example of a centralized virtual currency. Decentralized virtual currencies have no central repository and no single administrator. Instead, value is electronically transmitted between parties without an intermediary. Bitcoin is an example of a decentralized virtual currency. Bitcoin is also known as a cryptocurrency, meaning that it relies on cryptographic

software protocols to generate the currency and validate transactions (http://www.fincen.gov/news_room/testimony/html/20131119.html).

The development of virtual currencies is an attempt to meet a legitimate market demand. According to a Federal Reserve Bank of Chicago economist, U.S. consumers want payment options that are versatile and that provide immediate finality.

No U.S. payment method meets that description, although cash may come closest. Virtual currencies can mimic cash's immediate finality and anonymity and are more versatile than cash for online and cross-border transactions, making virtual currencies vulnerable for illicit transactions. Decentralized convertible virtual currency such as Bitcoin is still a niche payments product. The total 24- hour transfer volume for the top 10 Bitcoin exchangers was $22,995,398, averaging $249/transaction (Crypto-Currency Market Capitalizations. Available at http://coinmarketcap.com/).

SECTION 3 INSURANCE COMPANIES

Life, health, and accident insurance generate more than half a trillion dollars in premiums and contract revenue annually for U.S. insurers. Much of this revenue stream actually comes from the sale of annuities. In fact, according to the National Association of Insurance Commissioners (NAIC), "the primary business of life/health insurance companies is no longer traditional life insurance, but the underwriting of annuities; contracts that guarantee a fixed or variable payment over a given period of time." (NAIC, Life Insurance — Facts and Statistics. Accessed at: http://www.iii.org/media/facts/statsbyissue/life/).

Production Culture

A culture that focuses almost exclusively on production and income can motivate undesirable sales and underwriting practices if appropriate risk management systems are not in place.

Policy Cash Out

While whole and term life insurance policies remain an important part of the business, insurance agents and brokers are now often investment advisers selling a variety of financial products. The expansion from insurance policies to investment products has substantially increased the money laundering threat posed by the insurance industry. Recently, life insurers have developed products that offer a variety of investment options generating fixed or variable returns. These investment products are marketed as part of a diversified portfolio, often with tax benefits. The introduction of investment products to the insurance portfolio has broadened the potential customer base for insurers and agents and has created new transaction patterns. For example, a client with traditional insurance coverage might have had the fixed monthly premium automatically debited from a bank account; now, with an eye toward investment returns, that same client could choose to invest varying amounts monthly, or a single lump sum, potentially delivering cash to the agent.

A number of money laundering methods have been used to exploit the insurance sector, primarily life insurance policies and annuity products. Money launderers exploit the fact that insurance products are often sold by independent brokers and agents who do not work directly for the insurance companies. These intermediaries may have little know-how or incentive to screen clients or question payment methods. In some cases, agents take advantage of their intermediary status to collude with criminals against insurers to perpetrate fraud or facilitate money laundering.

An insurance company may offer its products through a number of different distribution channels. Some insurers sell their products directly to the insured. Other companies employ agents, who may either be “captive” or independent. Captive agents represent only one insurance company; independent agents may represent a variety of insurance carriers. Insurance may also be purchased through third parties such as financial planners or investment advisors (all of whom must be licensed insurance agents). Some companies and agents offer policies via the Internet.

Vulnerabilities

Life insurance policies that can be cashed in are an inviting money laundering vehicle because criminals are able to put “dirty” money in and take “clean” money out in the form of an insurance company check. An alternative typology is to borrow against a life insurance policy that is funded with illicit proceeds. Similarly, annuity contracts allow a money launderer to exchange illicit funds for an immediate or deferred “clean” income stream. These vulnerabilities generally do not exist in products offered by property and casualty insurers, or by title or health insurers.

Even when insurers have AML guidance in place, agents who sell insurance policies and investment contracts often are not employed directly by the insurer or service provider, which can make it difficult for companies to ensure their AML policies and procedures are followed. Further complicating AML practices, the policyholder, or purchaser of an insurance contract, may not be the beneficiary or even the subject of the insurance coverage. The potential for multiple parties to be involved in a single contract makes it difficult to perform customer due diligence.

Policies May Vary

Money laundering through insurance has been generally confined to life insurance products although the actual typologies vary significantly. In one case, federal law enforcement agencies discovered Colombian drug cartels were using drug proceeds to buy life insurance policies, which were subsequently liquidated with the cash value transferred to an offshore jurisdiction. The cash surrender value of a life insurance policy is often much less than the amount invested because of liquidation penalties, particularly if the policy has only been in existence for a few years. But from the drug traffickers’ perspective, the liquidation penalty is, in effect, a cost of doing business (See United States v. The Contents of Account No. 400941058 at JP Morgan Chase Bank, New York, NY, Mag. Docket No. 02-1163 (SDNY 2002) (warrant of seizure)).

In a case conducted by Immigration & Customs Enforcement (ICE), illicit drug proceeds were used to purchase three term life insurance policies in Austin, Texas, followed

shortly afterward by an attempt to cash in the policies (See In the Matter of Seizure of the Cash Value and Advance Premium Deposit Funds, Case No. 2002-5506-00007 (W. D. Tex. 2002)).Federal law enforcement agencies report similar cases involving money laundering through the purchase of variable annuity contracts.

A major ICE investigation into Eagle Star Life, based in the Isle of Man, with an office in Miami, was identified through information received in a narcotics smuggling investigation as issuing policies paid for with drug proceeds. The suspicious policies were established from 1995 through 2003 by one “master broker” who operated in Colombia and other South American countries. The policies were funded in several ways. In many instances, a large wire transfer was sent to the insurer on instructions from the broker. Once received, the broker would direct the allocation of funds to various policies. Eagle Star also received payments via third-party checks and structured money orders. Most alarming is evidence that some policies were paid for with funds from brokers’ commission accounts. In this scenario, the brokers accepted cash from the client in Colombia and credited the client’s policy with funds from the brokers’ business operating account or from commission checks.

Regulation and Public Policy

The insurance industry in the United States is currently subject to state rather than federal regulation. State regulation focuses primarily on safety and soundness rather than AML. However, FinCEN, pursuant to the BSA, promulgated AML regulations for the industry.

States oversee the organization and capitalization of insurance companies, permissible investments, licensing of companies and agents, and the form and content of policies. However, there is no consistency across the state regulatory regimes. States vary on how examinations are structured, how many examinations are performed, and how examiners are trained. As a result, states report they find it difficult to depend on other states’ oversight of companies’ market behavior (United States General Accounting Office, Insurance Regulation: Preliminary Views on States’ Oversight of Insurers’ Market Behavior, GAO-03-738T).

Some states have subjected insurance companies to AML statutes. According to an unpublished survey conducted by the National Association of Insurance Carriers, thirty-eight states have money laundering statutes, twenty-one have currency reporting requirements, and one has a suspicious activity reporting requirement (67 FR 64067).

FinCEN issued two sets of final rules for the insurance industry in 2005, the first covering minimum standards for AML programs and the second covering suspicious activity reporting requirements (Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations -- Anti-Money Laundering Programs for Insurance Companies, RIN 1506-AA70, Nov. 3, 2005 and Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations- Requirement That Insurance Companies Report Suspicious Transactions, RIN 1506-AA36, Nov. 3, 2005). The final rules apply to insurance companies that issue or underwrite certain products that present a high degree of risk for money laundering or the financing of terrorism or other illicit activity. The insurance products subject to these rules include:

- Permanent life insurance policies, other than group life insurance policies;
- Annuity contracts, other than group annuity contracts; and

- Any other insurance products with cash value or investment features.

The AML rule requires insurance companies offering covered insurance products to establish programs that include, at a minimum, the development of internal policies, procedures, and controls; the designation of a compliance officer; and ongoing employee training program; and, an independent audit function.

FinCEN's View on Agents and Brokers

The agent or broker will often be in a critical position of knowledge as to the source of investment assets, the nature of the clients, and the objectives for which the insurance products are being purchased. Agents and brokers have an important role to play in assisting the insurance company to prevent money laundering. Therefore, the final rule requires each insurance company to integrate its agents and brokers into its anti-money laundering program and to monitor their compliance with its program. The final rule also requires an insurance company's anti-money laundering program to include procedures for obtaining relevant customer-related information necessary for an effective program, either from its agents and brokers or otherwise.

The insurance company remains responsible for the conduct and effectiveness of its anti-money laundering program, which includes the activities of the agents and brokers that are involved with covered products. The insurance company must exercise due diligence, not only in the development of its anti-money laundering program and in the collection of appropriate customer and other information but also in monitoring the operations of its program, its employees, and its agents.[2]

SECTION 4 OPERATION CAPSTONE

The following case details how Columbian cocaine traffickers used life insurance policies to launder their drug profits.

"Operation Capstone" Cracks Sophisticated $80 Million Money Laundering Scheme that Exploited the International Life Insurance Industry

Multinational investigation marks the first time that massive drug money laundering through the life insurance industry has been exposed

WASHINGTON, D.C. - In the first investigation of its kind, authorities from the United States, the Isle of Man, and Colombia exposed a sophisticated criminal scheme that targeted life insurance companies in the United States, the Isle of Man, and other locations to launder some $80 million worth of Colombian drug proceeds over the span of several years The investigation took place from 2000-2002. Compiled from U.S. Customs and Border Protection news releases.

[2] Source: FinCEN October 2005

The Players, the Probe

Called "Operation Capstone," the two-year investigation was spearheaded by the U.S. Customs Service, the U.S. Attorney for the Southern District of Florida, the Isle of Man Customs & Excise Service, and Colombia's Departamento Administrativo de Seguridad (DAS). Her Majesty's Customs & Excise Service (U.K.), Panamanian authorities, and several police departments in South Florida also played critical roles in the case (which was alternatively known as "Operation Basking" in the Isle of Man and as "Operation Fan" in Colombia).

The probe revealed that Colombian drug trafficking organizations, through a small number of insurance brokers, were purchasing investment-grade life insurance policies in the United States, the Isle of Man, and other locations, with cartel associates as the beneficiaries. These policies were funded with tens of millions of dollars worth of drug proceeds sent (in the form of checks and wire transfers) to insurance companies by third parties around the globe.

Once an investment-grade life insurance policy is created, it operates much like a mutual fund. As such, customers can over-fund the policy beyond its face value and make early withdrawals, albeit with substantial penalties. Operation Capstone revealed that cartels were routinely liquidating their drug-financed life insurance policies after relatively short periods of time. The reason is that, despite paying stiff financial penalties for early liquidation, the cartel beneficiaries would receive a check or wire transfer from the insurance company that, on its surface, appeared to be legitimate insurance / investment proceeds. The cartels could then use these "clean" funds virtually unquestioned.

Operation Capstone resulted in numerous enforcement actions around the globe. U.S. Customs agents in Miami seized approximately $9.5 million during the course of the investigation. In addition, the Colombian DAS arrested 9 individuals in Colombia and seized roughly $20 million worth of insurance policies, bonds, and cash. Shortly after the Colombian arrests and seizures, Panamanian authorities froze $1.2 million in local accounts based on evidence uncovered in Colombia.

In another part of the case, a grand jury indicted 5 Colombian nationals on money laundering violations. Arturo Delgado, Jaime Eduardo Rey Albornoz, Alexander Murillo, Rodrigo Jose Murillo, and Esperanza Romero were accused of laundering approximately $2 million worth of drug proceeds through insurance companies.

Authorities in the United States, the Isle of Man, Colombia, and other jurisdictions identified more than 250 insurance policies that were linked to drug proceeds. Kenneth Dam, Deputy Secretary of the U.S. Treasury Department, said: "This investigation demonstrates that insurance companies, like other financial institutions, are susceptible to abuse by criminal organizations. The money laundered through insurance companies in this case constituted proceeds from illegal drug operations, but could have just as easily been money to finance terrorism. The new regulations that have been proposed by the Treasury Department are an important step towards closing down this enormous loophole."

The Global Investigation

Operation Capstone stemmed from a prior long-term investigation into the drug and money laundering activities of the Colombian cartels. During that investigation, U.S. Customs agents in Miami learned that these organizations were laundering large volumes of drug money through the purchase of life insurance policies in Europe, the United States, and offshore jurisdictions. Based upon this information, Customs agents in Miami launched Operation Capstone in late 2000. Customs agents identified life insurance policies in the Isle of Man, the United States, and elsewhere that were believed to be purchased with drug proceeds. At the same time, the Isle of Man Customs & Excise Service launched an independent, but parallel investigation (called Operating Basking) pursuant to the Island's anti-money laundering laws. When U.S. Customs and Isle of Man Customs & Excise became aware of their mutual targets, they merged their cases and pooled resources. In the summer of 2001, U.S. Customs agents began working closely with the Colombian DAS, which then launched an investigation of this scheme in their country. Customs agents and officials from the Colombian DAS discovered a network of Colombian insurance brokers who were working on behalf of the cartels and exploiting life insurance companies around the globe to launder narcotics proceeds. Ultimately, authorities from the United States, the Isle of Man, and Colombia merged their cases.

General Findings

During the course of the inquiry, investigators found that independent insurance sales brokers operating internationally had little or no training in anti-money laundering issues and were easily manipulated to place funds into non-bank financial institutions. The primary focus of the brokers in this case was selling insurance policies, often overlooking potential signs of money laundering by customers, such as a lack of explanation for wealth or unusual methods for the payment of premiums. Investigators also found that the insurance brokers in this case had a great deal of freedom and control over policies. These brokers often maintained pre-signed payment instructions for early withdrawals, allowing customers to withdraw funds with a telephone call. In addition, the brokers often paid premiums out of their own accounts and were reimbursed by the policyholder, often in cash. In some cases, the insurance brokers orchestrated payments into and out of a policy without the knowledge of the policyholder.

Furthermore, investigators found that there was limited oversight by the insurance companies in this case over their many brokers and sub-brokers. This, in turn, led to a breakdown in "know your customer" and "know your broker" regimes. The insurance companies in this case had little reliable information about some of their customers who had purchased policies through these brokers and sub-brokers. Investigators also found that legal requirements for insurance companies differed greatly from jurisdiction to jurisdiction. As a result of this situation and deficiencies in the global correspondent banking system, these insurance companies failed to recognize potential indicators of money laundering, such as payment of premiums via third parties, via currency exchange houses, or in the form of consecutively numbered checks and money orders. The probe disclosed that cartels were routinely liquidating their drug-financed life insurance policies early, despite the stiff financial penalties for early liquidation. The reason is that, despite the early withdrawal fees, the cartel beneficiaries would then receive funds from the insurance company that appeared to be legitimate insurance / investment proceeds.

SECTION 5 DEPT OF THE TREASURY 31 CFR Part 103

I. Background

In October 2001, President Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Public Law 107-56) (the Act). Title III of the Act makes a number of amendments to the anti-money laundering provisions of the Bank Secrecy Act. It requires every financial institution to establish an anti-money laundering program that includes, at a minimum,

(i) The development of internal policies, procedures, and controls;
(ii) The designation of a compliance officer;
(iii) An ongoing employee training program; and
(iv) An independent audit function to test programs

FinCEN published anti-money laundering final rules in October, 2005. The rules require that certain insurance companies establish an anti-money laundering program. The development of risk-based controls requires that each company assess the risk factors evident in the manufacture and sale of its products, and design and implement tailored controls appropriate to the level of risk. Risk factors must include an assessment of the company's products, customers, distribution methods, geographies being served, payment options and administrative operations. The AML program must include policies, procedures and internal controls that detect suspicious activity and provide for reporting of this detected activity to FinCEN in accordance with regulatory requirements. Agents and brokers do not have direct obligations under the final rules. However, insurance companies must integrate the company's agents and brokers into the compliance program, including the implementation of all relevant policies, procedures, training and monitoring.

Regulations Prescribed

Section 352(c) of the Act directs the Secretary to prescribe regulations for anti-money laundering programs that are "commensurate with the size, location, and activities" of the financial institutions to which such regulations apply. Section 5318(h)(1) permits the Secretary to exempt from this anti-money laundering program requirement those financial institutions not currently subject to FinCEN's regulations implementing the BSA. Section 5318(a)(6) of the BSA further provides that the Secretary may exempt any financial institution from any BSA requirement. Taken together, these provisions authorize the issuance of anti-money laundering program regulations that may differ with respect to certain kinds of financial institutions, and that may exempt certain financial institutions (and, by extension, certain financial institutions within the same industry) from the requirements of section 5318(h)(1). Although insurance companies have long been defined as a financial institution under the BSA, 31 U.S.C. 5312(a)(2)(M), FinCEN has not previously defined the term or issued regulations regarding insurance companies.

Insurance Company Regulation and Money Laundering- Explanation of Final Ruling

The statutory mandate that all financial institutions establish anti-money laundering programs is a key element in the national effort to prevent and detect money laundering and the financing of terrorism. The mandate recognizes that financial institutions other than depository institutions, which have long been subject to Bank Secrecy Act requirements, are also vulnerable to money laundering. The application of anti-money laundering measures to non-depository institutions generally, and to insurance companies in particular, also has been emphasized by the international regulatory community as a key element in combating money laundering. One of the central recommendations of the Financial Action Task Force, of which the United States is a member, is that financial institutions, including insurance companies, establish anti-money laundering programs. The Financial Action Task Force is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering. Originally created by the G-7 nations, its membership includes 36 nations, the European Commission, and the Gulf Cooperation Council.

This final rule applies only to insurance companies offering covered products, as defined in the rule. Insurance companies offer a variety of products aimed at transferring the financial risk of a certain event, from the insured to the insurer. These products include life insurance policies, annuity contracts, property and casualty insurance policies, and health insurance policies. These products are offered through a number of different distribution channels. Some insurance companies sell their products through direct marketing in which the insurance company sells a policy directly to the insured. Other companies employ agents, who may either be captive or independent. Captive agents generally represent only one insurer or one group of affiliated insurance companies; independent agents may represent a variety of insurance carriers. A customer also may employ a broker (i.e., a person who searches the marketplace for insurance in the interest of the customer) to obtain insurance.

This final rule focuses on those covered insurance products possessing features that make them susceptible to being used for money laundering or the financing of terrorism. For example, life insurance policies that have a cash surrender value are potential money laundering vehicles. Cash value can be redeemed by a money launderer or can be used as a source of further investment of tainted funds for example, by taking out loans against such cash value. Similarly, annuity contracts also pose a money laundering risk because they allow a money launderer to exchange illicit funds for an immediate or deferred income stream or to purchase a deferred annuity and obtain clean funds upon redemption. These risks do not exist to the same degree in term life insurance products, group life insurance products, group annuities, or in insurance products offered by property and casualty insurers or by title or health insurers. The international community has focused on life insurance policies and those insurance products with investment features as the appropriate subjects of anti-money laundering programs for insurance companies.

A review of the Suspicious Activity Reports filed with the Financial Crimes Enforcement Network reveals instances in which financial institutions have reported the suspected use of insurance products for the purpose of laundering the proceeds of criminal activity. During the few five years, a number of Suspicious Activity Reports were filed

that reference the use of an insurance product in suspected money laundering activity. For example, several reports describe as suspicious the large, lump-sum purchase of annuity contracts, followed almost immediately by several withdrawals of those funds. In some cases, the entire balance of the annuity contract was withdrawn shortly after the purchase of the contract. Other reports detail suspicious loans taken out against an annuity contract and life insurance premiums being paid by unrelated third parties.

Notice of Proposed Rulemaking

On September 26, 2002, the federal register published a notice of proposed rulemaking, 67 FR 60625, which would extend the requirement to establish an anti-money laundering program to insurance companies. The comment period for the proposed rule ended on November 25, 2002. The federal government received over 50 comments from insurance companies and agents, banks, trade associations, attorneys, and a government agency addressing issues raised by either the proposed rule or by a related proposed rule, 67 FR 64067 (October 17, 2002), that would require insurance companies to report suspicious transactions.

Summary of Comments

Most of the comments focused on the following matters:
(1) The potential application of an anti-money laundering program requirement to agents and brokers of insurance companies, rather than just their insurance company principals;
(2) the training of agents and brokers concerning their responsibilities under an insurance company's anti-money laundering program;
(3) the appropriate scope of the products that cause an entity to be defined as an insurance company for purposes of the rule.

These comments are discussed below. Other significant comments are discussed in the section-by-section analysis.

A. Treatment of Agents and Brokers

In the proposed rule, the federal government proposed that an insurance company, but not its agents or brokers, establish an anti-money laundering program. Under the proposed rule, an insurance company would be responsible for obtaining customer information from all relevant sources, including from its agents and brokers, necessary to make its anti-money laundering program effective. The federal government specifically sought comments on whether an insurance company's agents and brokers should be subject to a direct obligation to establish anti-money laundering programs. Commenters were almost evenly divided on this issue. Several agreed with the approach taken in the proposed rule, stating that the benefit of requiring tens of thousands of insurance agents and brokers to independently establish an anti-money laundering program would be outweighed by the costs. Other commenters argued that a direct obligation is necessary because insurance companies lack sufficient control over their distribution channels to integrate these elements into an adequate anti-money laundering compliance program. After careful consideration of all the views expressed, the government adopted the approach set forth in the proposed rule. Under the terms of the final rule, the obligation to establish an anti-money laundering program applies to an

insurance company, and not its agents or brokers. Certain agents of insurance companies are required under separate rules to establish anti-money laundering programs.

Nevertheless, because insurance agents and brokers are an integral part of the insurance industry due to their direct contact with customers, the final rule requires each insurance company to establish and implement policies, procedures, and internal controls reasonably designed to integrate its agents and brokers into its anti-money laundering program and to monitor their compliance with its program. An insurance company's anti-money laundering program also must include procedures for obtaining all relevant customer-related information necessary for an effective program, either from its agents and brokers or from other sources.

The final rule imposes a direct obligation only on insurance companies, and not their agents or brokers, for a number of reasons. First, whether an insurance company sells its products directly or through agents, the federal government believes that it is appropriate to place on the insurance company, which develops and bears the risks of its products, the responsibility for guarding against such products being used to launder unlawfully derived funds or to finance terrorist acts. Second, insurance companies, due to their much larger size relative to that of their numerous agents and brokers, are better able to bear the costs of compliance connected with the sale of their products. Although some agents work within large structures, only a small fraction of agencies employ more than a handful of people. According to one commenter, there are ''independent agents who operate on their own or in offices with just a few of their independent agent colleagues and thus comprise the quintessential notion of a small business operation.'' (Letter from the American Council of Life Insurers, Nov. 25, 2002)

Effectiveness of the Program as Implemented

If it appears that the effectiveness of the rule is being undermined by the failure of agents and brokers to cooperate with their insurance company principals, the government will consider proposing appropriate amendments to the rule. The federal government also expects that an insurance company, when faced with a non-compliant agent or broker, will take the necessary actions to secure such compliance, including, when appropriate, terminating its business relationship with such an agent or broker. Numerous insurers already have in place compliance programs and best practices guidelines for their agents and brokers to prevent and detect fraud. The government believes that insurance companies largely will be able to integrate their anti-money laundering programs into their existing compliance programs and best practices guidelines. Insurance agents and brokers will play an important role in the effective operation of an insurance company's anti-money laundering program. By refraining from placement of an independent regulatory obligation on agents and brokers, the federal government does not intend to minimize their role and intends to assess the effectiveness of the rule on an ongoing basis.

B. Training of Agents and Brokers

Several commenters requested that the final rule incorporate some flexibility regarding an insurance company's training of its agents and brokers. At least one commenter suggested that the government add language to the rule to avoid the duplicative training of independent agents that sell products on behalf of more than one insurance company.

The federal government agrees with these comments. Consequently, the final rule gives an insurance company the flexibility of directly training its agents and brokers. Alternatively, an insurance company may satisfy its training obligation by verifying that its agents and brokers have received the training required by the rule from another insurance company or from a competent third party with respect to the covered products offered by the company. Such training courses are already being developed and offered. A competent third party can include another financial institution that is required to establish an anti-money laundering program. For example, variable life insurance contracts and variable annuities (variable insurance products) are securities under the Securities Exchange Act of 1934 and therefore may be sold only by registered broker-dealers, who are required to have anti-money laundering programs pursuant to rules issued by the Financial Crimes Enforcement Network and the National Association of Securities Dealers and the New York Stock Exchange, two of the securities industry's self-regulatory organizations. In addition, other covered products, including fixed annuities, are sold by banks, which are also subject to anti-money laundering program requirements.

It is left to the discretion of an insurance company to determine whether the training of its agents by another party is adequate. The government does not intend to certify, license, or otherwise prospectively approve training programs.

C. Covered Products

Under the proposed rule, the issuing, underwriting, or reinsuring of a life insurance policy, an annuity contract, or any product with investment or cash value features, would have caused an insurance company to fall within the scope of the rule. A company that offered exclusively other kinds of insurance products, such as a property and casualty insurance policy, would not have been required to establish an anti-money laundering program. The overwhelming majority of commenters agreed with the distinction that the government made between higher-risk and lower risk insurance products. According to the *Joint Letter from the Independent Insurance Agents and Brokers of America and the National Association of Professional Insurance Agents,* Nov. 25, 2002, at 1- ''This distinction [between life insurance and property and casualty insurance] is legitimate and provides relief from the administrative and regulatory burdens of the proposed rule for the segments of the insurance industry that are at very low risk of money laundering.''

Some of those commenters requested that the federal government take the additional step of further excluding other kinds of insurance contracts and products relating to life insurance and annuities, such as reinsurance, group life insurance policies, group annuities, and term life insurance policies. The government, not having been informed or otherwise having learned of examples to the contrary, agree that some of these contracts and products pose little or no risk of being used for money laundering.

For example, reinsurance and retrocession contracts and treaties are arrangements between insurance companies by which they reallocate risks within the insurance industry and do not involve transactions with customers. Similarly, group life insurance policies and group annuities are typically issued to a company, financial institution, or association, and generally restrict the ability of an individual insured or participant to manipulate their investment. These products pose low money laundering risks.

Consequently, the final rule does not include in its coverage reinsurance or retrocession contracts or treaties, group life insurance, or group annuities. After careful consideration of the comments, the government also has decided to exclude term life (which includes credit life) insurance policies at this time. Given the operating characteristics of these products—e.g., the absence of a cash surrender value and the underwriting scrutiny given to term policies, especially those with large face amounts—the federal government believes that it would be impractical to launder money through term life insurance policies, and that the corresponding money laundering risks associated with such products are not significant. Nevertheless, as with all new exclusions, the position of the government will be reconsidered if circumstances warrant. While some insurance companies that offer a diversity of insurance products may decide to adopt company-wide anti-money laundering programs, regardless of the kinds of products they offer, the federal government wishes to emphasize that the final rule does not require that an insurance company adopt a companywide anti-money laundering program applicable to all of its insurance products. The anti-money laundering program requirement applies only to covered products, as defined in the final rule, offered by the insurance company.

II. Section-by-Section Analysis

Section 103.137(a) defines the key terms used in the rule. The definition of an insurance company reflects Treasury's determination that an anti-money laundering program requirement should be imposed on those sectors of the insurance industry that pose the most significant risk of money laundering and terrorist financing. The definition of an insurance company therefore includes any person engaged within the United States as a business in:

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

The sectors of the insurance industry offering life insurance and annuity products are both covered by the definition. The last category incorporates a functional approach, and encompasses any business offering currently, or in the future, any insurance product with an investment feature, and any insurance product possessing both stored value and transferability. The definition of an insurance company includes any person engaged "as a business" in the issuing, underwriting, or reinsuring of certain insurance products, and therefore does not include charities or other non-profit organizations.

The definition of an insurance company does not include insurance agents or brokers, as FinCEN believes the insurance company is in the best position to design an effective anti-money laundering program for its products, based upon the risk assessment it must perform due to the nature of its business. Agents and brokers would therefore not be required under the rule to independently establish an anti-money laundering program. However, as explained in greater detail below, an insurance company would be required to assess the money laundering and terrorist financing risks posed by its distribution channels and to incorporate policies, procedures, and internal controls integrating its agents and brokers into its anti-money laundering program.

Section 103.137(b) requires that each insurance company develop and implement an anti-money laundering program reasonably designed to prevent the insurance company from being used to facilitate money laundering or the financing of terrorist activities. The program must be in writing and must be approved by senior management. An insurance company's written program also must be made available to the Department of the Treasury or its designee upon request. The minimum requirements for the anti-money laundering program are set forth in section 103.137(c). Beyond these minimum requirements, however, the proposed rule is intended to give insurance companies the flexibility to design their programs to meet their specific risks.

Section 103.137(c) sets forth the minimum requirements of an insurance company's anti-money laundering program. Section 103.137(c)(1) requires the anti-money laundering program to incorporate policies, procedures, and internal controls based upon the insurance company's assessment of the money laundering and terrorist financing risks associated with its products, customers, distribution channels, and geographic locations. As explained above, an insurance company's assessment of customer-related information, such as methods of payment, is a key component to an effective anti-money laundering program. Thus, an insurance company's anti-money laundering program must ensure that the company obtains all the information necessary to make its anti-money laundering program effective. Such information includes, but is not limited to, relevant customer information collected and maintained by the insurance company's agents and brokers. The specific means to obtain such information is left to the discretion of the insurance company, although Treasury anticipates that the insurance company may need to amend existing agreements with its agents and brokers to ensure that the company receives necessary customer information.

For purposes of making the required risk assessment, an insurance company must consider all relevant information. The following are just some of the many factors that should be considered by an insurance company when making its risk assessment: whether the company permits customers to use cash or cash equivalents to purchase an insurance product, whether the company permits customers to purchase an insurance product with a single premium or lump-sum payment, and whether the company permits customers to take out a loan against the value of an insurance product. Other factors that should be considered include whether the insurance company engages in transactions involving a jurisdiction whose government has been identified by the Department of State as a sponsor of international terrorism under 22 U.S.C. 2371, has been designated as non-cooperative with international anti-money laundering principles, or has been designated by the Secretary of the Treasury as warranting special measures due to money laundering concerns.

Policies, procedures, and internal controls also must be reasonably designed to ensure compliance with BSA requirements. Insurance companies going forward are required to comply with BSA requirements regarding accountholder identification and verification pursuant to section 326 of the Act, as well as the filing of suspicious activity reports. As insurance companies become subject to additional BSA requirements, their compliance programs will obviously have to be updated to include appropriate policies, procedures, training, and testing functions. Insurance companies typically conduct their operations through agents and third-party service providers. Some elements of the compliance program will best be performed by personnel of these entities, in which case it is permissible for an insurance company to delegate contractually the implementation and operation of those aspects of its anti-money laundering program to such an entity.

Delegation, Designation and Compliance

Any insurance company that delegates responsibility for aspects of its anti-money laundering program to an agent or a third party, however, remains fully responsible for the effectiveness of the program, as well as ensuring that federal examiners are able to obtain information and records relating to the anti-money laundering program and to inspect the agent or the third party for purposes of the program. In addition, an insurance company remains responsible for the following:

- assuring compliance with this regulation
- taking reasonable steps to identify the aspects of its operations that may give rise to BSA regulatory requirements or that are vulnerable to money laundering or terrorist financing activity
- developing and implementing a program reasonably designed to achieve compliance with such regulatory requirements and to prevent such activity
- monitoring the operation of its program
- assessing the effectiveness of its program

For example, it would not be sufficient for an insurance company simply to obtain a certification from its delegate that the company "has a satisfactory anti-money laundering program."

Section 103.137(c)(2) requires that an insurance company designate a compliance officer to be responsible for administering the anti-money laundering program. An insurance company may designate a single person or committee to be responsible for compliance. The person or persons should be competent and knowledgeable regarding BSA requirements and money laundering issues and risks, and should be empowered with full responsibility and authority to develop and enforce appropriate policies and procedures. The role of the compliance officer is to ensure that-

(1) the program is being implemented effectively
(2) the program is updated as necessary; and
(3) appropriate persons are trained and educated in accordance with section 103.137(c)(3).

Education and Training

Section 103.137(c)(3) requires that an insurance company provide for education and training of appropriate persons. Employee training is an integral part of any anti-money laundering program. In order to carry out their responsibilities effectively, employees of an insurance company (and of any agent or third-party service provider) with responsibility under the program must be trained in the requirements of the rule and money laundering risks generally so that "red flags" associated with existing or potential customers can be identified. Such training could be conducted by outside or in-house seminars, and could include computer-based training. The nature, scope, and frequency of the education and training program of the insurance company will depend upon the functions performed. However, those with obligations under the anti-money laundering program must be sufficiently trained to carry out their responsibilities effectively. Moreover, these employees should receive periodic updates and refreshers regarding the anti-money laundering program.

Section 103.137(c)(4) requires that an insurance company provide for independent testing of the program on a periodic basis to ensure that it complies with the requirements of the rule and that the program functions as designed. An outside consultant or accountant need not perform the test. An employee of the insurance company may perform the independent testing, so long as the tester is not the compliance officer or otherwise involved in administering the program. The frequency of the independent testing will depend upon the insurance company's assessment of the risks posed. Any recommendations resulting from such testing should be implemented promptly or reviewed by senior management.

Section 103.137(d) states that an insurance company that is registered or is required to register with the Securities and Exchange Commission (SEC) shall be deemed to have satisfied the requirements of this section for those activities regulated by the SEC to the extent that the company complies with the anti-money laundering program requirements applicable to such activities that are imposed by the SEC or by a self-regulatory organization (SRO) registered with the SEC. Thus, for example, an insurance company that is required to register as a broker-dealer in securities because it sells variable annuities may satisfy the anti-money laundering program requirements under the proposed rule for that activity by complying with the anti-money laundering program requirements applicable to such activity that are imposed by the SEC or one of its registered SROs. To the extent that the issuance of annuities, or any other activity by an insurance company, is not covered by an SEC or SRO-anti-money laundering program rule, then such activity would be subject to the anti-money laundering program requirements of rule.

SECTION 6 AML POLICY EXAMPLE

This chapter is an example of an anti-money laundering policy as promulgated by the 'XYZ' Insurance Company. Familiarity with this prototype policy and grounding in know-your-customer concepts are pillars in money laundering awareness.

POLICY STATEMENT AND PRINCIPLES

In compliance with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) ("Act"), Pub. Law 107-56(2001), XYZ Insurance Companies ("XYZ") have adopted an Anti-Money Laundering (AML) compliance policy ("Policy") as set forth in the Board minutes of its respective life insurance companies, dated September 2002 and updated May 2006; to incorporate the Final Rules issued by Financial Crimes Enforcement Network ("FinCEN") United States Department of the Treasury ("Treasury") in November 2005.

SCOPE OF POLICY

This policy applies to all XYZ Insurance Companies ("XYZ"), its officers, employees, appointed producers and products and services offered by XYZ. All business units, including, without limitation, the XYZ Annuity Group, and locations within XYZ will cooperate to create a cohesive effort in the fight against money laundering. Each business unit and location have implemented risk-based procedures reasonably expected to prevent, detect and cause the reporting of transactions required under Title

III, Section 352 and Section 326, of the Act. All efforts exerted will be documented and retained in accordance with the Act. The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee.

POLICY

It is the policy of XYZ to actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. XYZ is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes.

For the purposes of the Policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

AML COMPLIANCE COMMITTEE

The AML Compliance Committee, with full responsibility for the Policy shall be comprised of the General Counsel, XYZ Financial Group ("XYZ Fin Group"); Chief Compliance Officer, XYZ; Deputy Compliance Officer, XYZ; Assistant Vice President-Internal Audit, and Corporate Attorney-XYZ Life Insurance Company. The Chief Compliance Officer shall also hold the title Chief AML Officer, and shall have authority to sign as such.

The duties of the AML Compliance Committee with respect to the Policy shall include, but are not limited to, the design and implementation of as well as updating the Policy as required; dissemination of information to officers, employees and appointed producers of XYZ, training of officers, employees and appointed producers; monitoring the compliance of XYZ operating units and appointed producers, maintaining necessary and appropriate records, filing of SARs when warranted; and independent testing of the operation of the Policy.

Each XYZ business unit shall appoint a contact person to interact directly with the AML Compliance Committee to assist the Committee with investigations, monitoring and as otherwise requested.

COVERED PRODUCTS
The final regulations define "covered products to include: (1) permanent life insurance policies, other than group life insurance; (2) annuity contracts, other than group annuity contracts; or (3) any other insurance products with features of cash value or investment.

The products offered through XYZ which meet the definition of a "covered product" include, but may not be limited to; fixed and variable universal life, whole life, and fixed and variable annuities.

CUSTOMER IDENTIFICATION PROGRAM
XYZ has adopted a Customer Identification Program (CIP). XYZ will provide notice that they will seek identification information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results; and compare customer identification information with OFAC.

Notice to Customers
XYZ will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law. The following notice will be used:
To help fight the funding of terrorism and money-laundering activities, the U.S. Congress has passed the USA PATRIOT Act, which requires financial institutions, including insurance companies, to obtain, verify and record information that identifies persons who engage in certain transactions with or through our company. This means that we will verify your name, residential or street address, date of birth and social security number of other tax identification number on the application. We may also ask to see a driver's license or other identifying documents from you.

Required Customer Information
The following information will be collected for all new insurance and annuity applications:

- Name,
- Date of birth,
- Address,
- Identification number, which will be a social security number ("SSN") or taxpayer identification number ("TIN") for U.S. persons or entities,
- Photo identification (drivers license or other comparable source) or;
- for non-U.S. persons or entities one or more of the following;
- Passport number and country of issuance,
- Alien identification card number or;
- Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

VERIFYING INFORMATION
Based on the risk, and to the extent reasonable and practicable, XYZ will ensure that it has a reasonable belief of the true identity of its customers. In verifying customer identity, appointed producers shall review photo identification.

XYZ shall not attempt to determine whether the document that the customer has provided for identification has been validly issued. For verification purposes, XYZ shall rely on a government-issued identification to establish a customer's identity. XYZ,

however, will analyze the information provided to determine if there are any logical inconsistencies in the information obtained.

XYZ will document its verification, including all identifying information provided by the customer, the methods used and results of the verification, including but not limited to sign-off by the appointed producer of matching photo identification.

Customers Who Refuse To Provide Information

If a customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the appointed agent shall notify their New Business team. The XYZ New Business team will decline the application and notify the AML Compliance Committee.

Checking the Office of Foreign Assets Control ("OFAC") List

For all (1) new applications received and on an ongoing basis, (2) disbursements (3) new producers appointed or (4) new employees, XYZ will check to ensure that a person or entity does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site. XYZ contracted with Acme Security Systems to ensure speed and accuracy in the checks. XYZ will also review existing policyholders, producers and employees against these lists on a periodic basis. The frequency of the reviews will be documented and retained.

In the event of a match to the SDN List or other OFAC List, the business unit will conduct a review of the circumstances where such match has been identified. If the business unit is unable to confirm that the match is a false positive, the AML Committee shall be notified.

MONITORING AND REPORTING

Transaction based monitoring will occur within the appropriate business units of XYZ. Monitoring of specific transactions will include but is not limited to transactions aggregating $5,000 or more and those with respect to which XYZ has a reason to suspect suspicious activity. All reports will be documented and retained in accordance with the Act.

SUSPICIOUS ACTIVITY

There are signs of suspicious activity that suggest money laundering. These are commonly referred to as "red flags." If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee.

Examples of red flags:

- The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force.
- The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer's account shows numerous currency or cashier’s check transactions aggregating to significant sums.
- The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S ("Reg S") stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- Attempt to borrow maximum cash value of a single premium policy soon after purchase.
-

If the appointed producer:

- Exhibits a dramatic or unexpected increase in sales (particularly of single premium contacts)
- Has consistently high activity in single premium contracts in excess of company averages
- Exhibits a sudden change in lifestyle
- Requests client documentation be delivered to the agent

INVESTIGATION

Upon notification to the AML Compliance Committee of a match to the OFAC SDN List or possible suspicious activity, an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to file a blocked assets and/or a SAR with the appropriate law enforcement or regulatory agency. The AML Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agency.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. **Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family. Disclosure of such is strictly prohibited by the Act.**

Information Sharing

XYZ are eligible to share information with other financial institutions under the USA PATRIOT Act for purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain a policy or engage in a transaction. The final rule (section 103.110) became effective Sept. 26, 2002. Registration with FinCEN is required prior to any information being shared between financial institutions. The AML Compliance Committee will register each XYZ with FinCEN individually to facilitate appropriate information sharing under the USA PATRIOT Act. The notice form found at www.fincen.gov will be used. XYZ will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information.

Recordkeeping

The AML Compliance Committee will be responsible to ensure that AML records are maintained properly and that SARs and Blocked Property Reports are filed as required. XYZ will maintain AML records for at least five years. The five-year retention period will be applied for five years after the policy or contract is surrendered, lapsed, terminated by death, or closed for any reason.

Training

XYZ contracted with Best Insurance Education to provide general AML training to its officers, employees and appointed producers to ensure awareness of requirements under the Act. The training will include, at a minimum: how to identify red flags and signs of money laundering; what roles the officers, employees and appointed producers have in the XYZ compliance efforts and how to perform such duties and responsibilities; what to do once a red flag or suspicious activity is detected; XYZ record retention policy; and the disciplinary consequences for non-compliance with the Act and this Policy.

In addition, each affected area will provide enhanced training in accordance with the procedures developed in each area for officers and employees reasonably expected to handle money, requests, or processing that may bring them into contact with information designated above.

A producer may be appointed with another insurance company or a broker-dealer subject to the AML requirements under Section 352 of the USA PATRIOT Act and have received other AML training. The XYZ AML Compliance Committee may rely upon such training as satisfying XYZ AML training requirements if it has been certified by the AML Compliance Officer or other appropriate authority of such other company as having been completed and such training includes the required core elements as determined by the AML Compliance Committee. In the event a producer receives training via a third party not subject to the AML requirements under Section 352 of the USA PATRIOT Act, XYZ AML Compliance Committee will determine whether such training meets the requirements of the XYZ AML training program.

Training will be conducted on an annual basis. The XYZ AML Compliance Committee will determine the ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training. XYZ will maintain records to document that training has occurred

Testing of the Policy

The testing of the Policy will be conducted by an outside independent third party in 2007 and annually thereafter. Any findings will be reported to the AML Compliance Committee, XYZ Fin Group Audit Committee and Senior Management for appropriate action.

ADMINISTRATION

The AML Compliance Committee is responsible for the administration, revision, interpretation, and application of this Policy. The Policy will be reviewed annually and revised as needed.

1. The Customer Identification Program shall be implemented by December 31, 2006.
2. The Customer Notice shall be incorporated by December 31, 2006.
3. Sign-off by appointed producer shall be required by December 31, 2006.
4. Initial training shall be completed by December 31, 2006 and annually thereafter.