

Life or Health Agents Only

Anti-Money Laundering Online Study Book

You Are On Page 1 — Use Your "Page Down" Button To Start Reading The Book



[Search The Book](#)

[Save This Book](#)

[Exam](#)

[Help / Instructions](#)

AE *AffordableEducators*
41890 Enterprise Cir So #100, Temecula, Ca 92590 (800) 498-5100

Copyright © D&H Investment Trust. Courses are provided with the understanding that we are not engaged in rendering legal or other professional advice unless we agree to this in writing, in advance. Insurance and financial matters are complicated and you need to discuss specific fact situations concerning your personal and client needs with an appropriate advisor before using any information from our courses.

Anti Money Laundering Online Study Book

You Are On Page 1 — Use Your "Page Down" Button To Start Reading The Book



[Search The Book](#)

[Save This Book](#)

[Exam](#)

[Help / Instructions](#)

AE Affordable Educators
41890 Enterprise Cir So #100, Temecula, Ca 92590 (800) 498-5100

Copyright © D&H Investment Trust. Courses are provided with the understanding that we are not engaged in rendering legal or other professional advice unless we agree to this in writing, in advance. Insurance and financial matters are complicated and you need to discuss specific fact situations concerning your personal and client needs with an appropriate advisor before using any information from our courses.

CONTENT

INTRODUCTION 3

MONEY LAUNDERING & THE INSURANCE INDUSTRY 4

History of money laundering	4
Money laundering, three stages	4
Three stages of money laundering	4
Definition, money laundering	5
Money laundering, definition	5
Insurance companies, target for ML	6
Money laundering, insurance a target	6
Vulnerabilities of insurance companies	6

MONEY LAUNDERING LEGISLATION & INSURANCE 9

Anti-money laundering regulations	9
Bank Secrecy Act 1970	9
Money laundering legislation	9
Financial institutions	10
HR 3199	10
USA Patriot Act	10
Money laundering legis & insurance	12
Agents and brokers, new AML rules	14
New anti-money laundering rules	14
New rules, agents & brokers	14
Suspicious Activity Reports	14
Anti-money laundering training	15
Red flags	17
Compliance	18
Compliance officer	18
SEC exemption	19
Violations of Bank Secrecy Act	19

FREQUENTLY ASKED QUESTIONS 20

FAQ's of anti-money laundering rule	20
Federal Crimes Enforcement Net	20
Covered products	21
Anti-money laundering requirements	22
Internal controls	23
Ongoing training	23
Monitoring an adequate program	24
Training of agents	24
Report of cash payments	25
Obligation to identify	26
Suspicious Activity Reports & agents	26

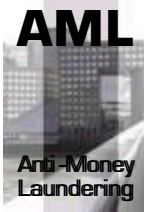
Civil liability	28
Disclosure, Suspicious Activity Rpt	28

ANTI-MONEY LAUNDERING CONTROLS & PROCEDURES 29

Anti-money laundering controls	29
Customer due diligence	29
Customer due diligence measures	30
Risk profile	30
Business relationship	31
Identification & verification	32
Timing of identification & verification	32
Transactions or trigger events	33
Transactions, trigger or attention	33
Identification & verification, methods	34
Methods of identification & verification	34
Legal persons and arrangements	35
Developing technologies	36
New technologies, difficult identity	36

INDICATORS & EXAMPLES OF INSURANCE MONEY LAUNDERING SCHEMES 37

Indicators & examples of AML	37
Life insurance	38
Non-life insurance	39
Intermediaries	40
Reinsurance	41
Claims	42
Overpayment of premiums	42
Return of premiums	42
Third party payments	42
Assignment of claims	43
Fraudulent claims	43
A final word to agents	45



INTRODUCTION

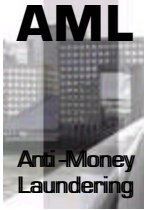
Money laundering has become a major priority for America's war on terrorist funding. Since 9/11, World banks and many industries prone to money laundering have revised procedures and now comply with many rules and regulations. HR 3199, the USA Patriot Act Improvement and Reauthorization Act of 2005, created new rules for **insurance companies** concerning anti-money laundering policies and training.

Insurers are now obligated to establish an anti-money laundering program, and, because insurance agents and brokers are an integral part of the insurance industry due to their direct contact with customers, the new rules **require** 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.

This course provides training agents can use to assess the money laundering risks inherent in insurance transactions and to identify potential "red flags".

HR 3199 specifically authorizes third-party anti-money laundering training stating that the "insurance company could generally rely on the agent's own program requirements to address issues at the time of the sale if reasonable (i.e., the insurer knows of no defect in the agent's program), while the insurer's program should focus on the ongoing administration of the covered product".

Registered Reps have, since 2002, been required to complete securities anti-money laundering programs. According to HR 3199, this training may not qualify for insurance training where "covered products" discussed do not address specified insurance products offered by the insurer. Thus, agents need the present course to be sure they are getting insurance-specific anti-money laundering information and training.



MONEY LAUNDERING & THE INSURANCE INDUSTRY

A Brief History of Money Laundering

The act of "money laundering" was first used during the prohibition era in the United States. Methods were devised to disguise the origins of money generated by the sale of then-illegal alcoholic beverages. Mobsters were known to transfer funds from New Orleans slot machines to accounts overseas or even buy Swiss banks where the transfer of illegal funds transpired through a complex system of shell companies, holding companies and offshore accounts.

The term of "money laundering" itself does not derive, as is often said, from the story that Al Capone used laundromats to hide ill-gotten gains. Actually, the first reference to the term "money laundering" itself appeared during the Watergate Scandal. US President Richard Nixon's "Committee to Re-Elect The President" moved illegal campaign contributions to Mexico, then brought the money back through a company in Miami. It was British newspaper (The Guardian) that coined the term, referring to the process as "laundering."

The 1980's witnessed the international trend for the criminalization of money laundering as a discrete crime. The US and the UK have done so in 1986, and the 1988 Vienna Convention has required State Parties to introduce this crime in their domestic legal systems

After 9/11, money laundering became a major concern for the US war on terror. Clearstream, "a bank of banks" which practice financial clearing, centralizing debit and credit operations for hundreds of banks, has been accused of being a major operator of the underground economy via a system of un-published accounts; Bahrain International Bank, owned by Oasma bin Laden, would have profited from these transfer facilities were it not for a scandal leading to the CEO of Clearstream to resign on December 31, 2001. Since then, several judicial investigations were opened to investigate the accusations and to ensure that an International response to the underground economy, money laundering and counter terrorism funding be coordinated by the Financial Action Task Force on Money Laundering (FATF). Compliance with, or a movement towards compliance with, the principals of this task force is now seen as a requirement of an internationally active bank or other financial service entity.

The Money Laundering Process

Money laundering is often described as occurring in **three stages**: placement, layering, and integration.

- **Placement:** refers to the initial point of entry for funds derived from criminal activities.
- **Layering:** refers to the creation of complex networks of transactions which attempt to obscure the link between the initial entry point and the end of the laundering cycle.
- **Integration:** refers to the return of funds to the legitimate economy for later extraction.

Example: If a person is making thousands of dollars in small change a week from his business (not unusual for a store owner), and he wishes to deposit that money in a bank, he cannot do so without possibly drawing suspicion. In the United States, for example, cash transactions and deposits of more than \$10,000 are required to be reported as "significant cash transactions" to the Financial Crimes Enforcement Network (FinCEN), along with any other suspicious financial activity as "suspicious activity reports". In other jurisdictions, suspicion based requirements are placed on financial services employees and firms, like insurance companies, to report suspicious activity to the authorities.

One method of keeping this small change private would be for an individual to give his money to an intermediary who is already legitimately taking in large amounts of cash. The intermediary would then deposit that money into his account, take a premium, and write a check to the individual. Thus, the individual draws no attention to himself, and can deposit his check into a bank account without drawing suspicion. This works fine for *one-off* transactions, but if it occurs on a regular basis then the check deposits themselves can form a paper trail and raise suspicion.

Another method involves establishing a business whose cash inflow cannot be monitored, and funneling the small change into this business and paying taxes on it. All bank employees however are trained to be constantly on the lookout for any transactions which appear to be an attempt to get around the currency reporting requirements. Such shell companies should deal directly with the public, perform some service related activity as opposed to providing physical goods, and reasonably accept cash as a matter of business.

Dealing directly with the public ensures plausible anonymity of source. An example of a legitimate business displaying plausible anonymity of source would be a gas station. Since it would be unreasonable for them to keep track of the identity of their customers, a record of their transaction amounts must be ostensibly accepted as *prima facie* evidence of actual financial activity. Service related businesses have the advantage of anonymity of resources. A business that sells computers has to account for where it actually got the computers, whereas a plumbing company merely has to account for fictitious labor. Reasonably accepting cash means the business must regularly perform services that total less than \$500 on average, since above that amount most people pay with a check, credit card, or other traceable payment method. The company should actually function on a legitimate level. In the plumbing company example, it is perfectly reasonable for a lot of the business to involve only labor (no parts), and for some business to be paid for in cash, but it is unreasonable for all of their business to involve no parts and only cash payment. Therefore the legitimate business will generate a legitimate level of parts usage, as well as enough traceable transactions to mask the illegitimate ones. It should be noted that each of the above examples is flawed in one or more ways and serves only to illustrate the specific feature being discussed. Gas stations are flawed because they would have to account for the actual gas they sold, plumbers usually provide warranties on their work, which necessarily includes the names and addresses of the customers.

By the strictest **definition** of the term, anyone who assists in concealing the proceeds from his transactions is considered a **money launderer**. An individual therefore may be unwittingly employed by money launderers, and may still be criminally liable in many jurisdictions. It should be noted, however, that the act of concealing money is different

from that of laundering it, though many make the mistake of putting both actions under the term of laundering.

Corrupt politicians and lobbyists also launder money by setting up personal non-profits to move money between trusted organizations so that donations from inappropriate sources may be illegally used for personal gain.

Money Laundering & Insurance

Although its vulnerability is not regarded to be as high as for other sectors of the financial industry, the insurance sector is a possible target for money launderers and for those seeking resources for terrorist acts or for ways to process funds to accomplices. Insurers can be involved, knowingly or unknowingly, in money laundering and the financing of terrorism. This exposes them to legal, operational and reputational risks. The insurance sector should therefore take adequate measures to prevent its misuse by money launderers and terrorists, and should address possible cases of money laundering and terrorist financing forthwith.

For these reasons and more, international organizations and U.S. legislation under the Patriot Act now include compliance among insurers who are expected to "integrate" agents in their anti-money laundering programs.

Why Would An Insurance Company Be A Target for Money Laundering?

Money launderers enjoy doing business with companies with a **large customer base**, increasing the potential for them to hide the real purpose behind their insurance purchases. Insurance companies provide insurance coverage to large segments of the of the total population, a significant pool of users within which to hide illegal transactions.

In addition, the value of assets throughout the industry make the insurance sector a logical place for investing significant amounts of illegal profits. The **security** of these investments through government bonds and real estate make it very appealing for those illegal profits to generate a sound return. Furthermore, the large number of investors ensures a significant level of transaction activity, thereby increasing the potential for money laundering to take place unnoticed. This makes a company's due diligence practices all the more important to ensure transactions do not slip between the cracks under the sheer volume of activity --- particularly around income tax filing season.

Finally, money laundering has no borders and companies that do business in **other jurisdictions** increase the risk that they will be targeted. Insurance companies do business in many countries, including the electronic transfer of funds. Established due diligence practices for these international transactions will have to be put in place and monitored, the failure to do so could result in criminal charges being laid against the company.

Money Laundering Vulnerabilities of Insurance Companies

Life insurance and non-life insurance can be used in different ways by money launderers and terrorist financiers. The vulnerability depends on factors such as (but not limited to) the complexity and terms of the contract, distribution, method of payment (cash or bank transfer) and contract law. Insurers should take these factors into account when

assessing this vulnerability. This means they should prepare a risk profile of the type of business in general and of each business relationship.

Examples of the type of life insurance contracts that are vulnerable as a vehicle for laundering money or terrorist financing are products, such as:

- Unit-linked or with profit single premium contracts
- Single premium life insurance policies that store cash value
- Fixed and variable annuities
- Endowment policies

When a life insurance policy matures or is surrendered, funds become available to the policyholder or other beneficiaries. The beneficiary to the contract may be changed – possibly against payment –before maturity or surrender, in order that payments are made by the insurer to a new beneficiary. A policy might be used as collateral to purchase other financial instruments. These investments in themselves may be merely one part of a sophisticated web of complex transactions with their origins elsewhere in the financial system.

Non-life insurance money laundering or terrorist financing can be seen through inflated or totally bogus claims, e.g. by arson or other means causing a bogus claim to be made to recover part of the invested illegitimate funds. Other examples include cancellation of policies for the return of premium by an insurer's check, and the overpayment of premiums with a request for a refund of the amount overpaid. Money laundering can also occur through under-insurance, where a criminal can say that he received compensation for the full amount of the damage, when in fact he did not.

Examples of how terrorism could be facilitated through property and casualty coverage, include use of worker's compensation payments to support terrorists awaiting assignment and primary coverage and trade credit for the transport of terrorist materials. This could also imply breach of regulations requiring the freezing of assets.

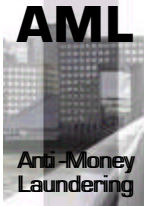
Money laundering and the financing of terrorism using reinsurance could occur either by establishing fictitious (re)insurance companies or reinsurance intermediaries, fronting arrangements and captives, or by the misuse of normal reinsurance transactions.

Examples include: the deliberate placement via the insurer of the proceeds of crime or terrorist funds with reinsurers in order to disguise the source of funds the establishment of bogus reinsurers, which may be used to launder the proceeds of crime or to facilitate terrorist funding the establishment of bogus insurers, which may be used to place the proceeds of crime or terrorist funds with legitimate reinsurers.

Insurance intermediaries, like adjusters, agents and brokers, are important for distribution, underwriting and claims settlement. They are often the direct link to the policyholder and therefore intermediaries should play an important role in anti-money laundering and combating the financing of terrorism. In essence, they are on the "front lines" of the anti-money laundering war and should be considered the best source for customer due diligence. The person who wants to launder money or finance terrorism may seek an insurance intermediary who is not aware of, or does not conform to, necessary procedures, or who fails to recognize or report information regarding possible

cases of money laundering or the financing of terrorism. The intermediaries themselves could be easily set up to channel illegitimate funds to insurers.

We will provide more, very specific examples of money laundering in the last section of this course so you may be alert to the conditions and indicators where illegal activity and possible terrorist funding may develop.



MONEY LAUNDERING LEGISLATION & INSURANCE

Regulations surrounding anti-money laundering in the United States center around two primary pieces of legislation:

- The Bank Secrecy Act of 1970
- USA Patriot Act: Title III

In one form or another, these acts issue regulations requiring financial institutions, including insurance companies, to keep records and file reports that are determined to have a high degree of usefulness in criminal, tax and regulatory matters, or in the conduct of intelligence or counter intelligence activities, including the determination of terrorism funding and money laundering programs.

The Bank Secrecy Act of 1970

The Bank Secrecy Act (BSA), enacted in 1970, authorizes the Secretary of the Treasury to issue regulations requiring that financial institutions keep records and file reports on certain financial transactions. The authority of the Secretary to administer Title II of the BSA (codified at 31 U.S.C. 5311-5330 with implementing regulations at 31 C.F.R. Part 103) has been delegated to the Director of the Financial Crimes Enforcement Network (FinCEN).

Hundreds of thousands of financial institutions are currently subject to BSA reporting and recordkeeping requirements, including depository institutions (e.g., banks, credit unions and thrifts); brokers or dealers in securities; money services businesses [MSBs (e.g., money transmitters; issuers, redeemers and sellers of money orders and travelers' checks; check cashers and currency exchangers)]; casinos and card clubs. Insurance companies were considered a financial institution, but not subject to reporting until 2002 (more on this later).

The Bank Secrecy Act, commonly referred to as **Title 31**, has been evolving since the original legislation was enacted in October 1970. The overall purpose of the act was to fight money laundering and other financial crimes by requiring financial institutions to report cash transactions in excess of \$10,000. Initially, this legislation focused on banking institutions. However, the law has been modified several times over the past three decades to expand the number and type of industries and transactions covered.

The Department of the Treasury recognized the importance of extending the counter-money laundering controls to 'non-traditional' financial institutions, not simply to banks, both to insure fair competition in the marketplace and to recognize that non-banks as well as depository institutions are an attractive mechanism for, and are threatened by, money launderers. For example, the definition of *financial institutions* has been expanded to include casinos (1985), Indian casinos (1996), and card rooms (1998).

Other businesses which fall under the definition of financial institutions are **money transmitters** and **money order and traveler's check issuers, sellers, and**

redeemers... The inclusion of suspicious transactions is one of a number of additional amendments made to the Bank Secrecy Act which went into effect on July 1, 1997." ¹

USA Patriot Act

The USA PATRIOT Act, enacted on October 26, 2001, has been critical, in the opinion of some, in preventing another terrorist attack on the United States. It brought the federal government's ability to investigate threats to the national security into the modern era—by modifying our investigative tools to reflect modern technologies, eliminating barriers to effective national security investigations, and giving national security investigators the same sorts of tools as have long been available to investigators who handle non-national security matters.

Recently, following intense debate, Congress passed the USA Patriot Act Improvement and Reauthorization Act of 2005 (**H.R. 3199**). This legislation **reauthorizes** all expiring provisions of the USA PATRIOT Act and adds dozens of additional safeguards related to privacy and civil liberties, and port security..

Title III of the USA Patriot Act focuses on beefing up U.S. money laundering defenses and changes those laws to help deal with terrorism. Highlights of the money laundering provisions in the law include:

1. Allows the Secretary of the Treasury to require increased record keeping and reporting by financial institutions (defined very broadly under 31 USC 5312 1) concerning transactions involving:

- Jurisdictions outside the United States,
- Financial institutions outside the United States, and/or
- Classes of transactions involving jurisdictions outside of the United States, that are considered by the Secretary to be a primary money laundering concern.

2. Requires special due diligence for correspondent accounts and private banking accounts involving foreign persons or financial institutions and prohibits U.S. financial institutions from establishing correspondent accounts with foreign shell banks with no physical presence.

3. Requires the Secretary of the Treasury to adopt regulations to encourage cooperation among financial institutions, their regulatory authorities, and law enforcement authorities to share information regarding individuals, entities and

Financial Institutions

Financial Institutions under the Patriot Act are defined as everything from (A) to (Z) including: a currency exchange; an issuer, redeemer or cashier of travelers' checks, checks, money orders, or similar instruments; an insurance company; a pawnbroker; a loan finance company; a dealer in precious metals, stones, or jewels; a travel agency; a licensed sender of money; a business engaged in vehicle sales, including automobiles, airplanes and boats; persons involved in real estate closings and settlements; and casinos...among other things.

¹ "Suspicious Transactions: A Continuation of the Bank Secrecy Act" by John R. Mills, Ph.D., and Janet M. Vreeland, Ph.D.

organizations engaged in terrorist acts or money laundering activities.

4. Includes foreign corruption offenses as money laundering crimes.
5. Allows for forfeiture of funds from United States interbank accounts up to the amount of the funds deposited in a foreign bank with no requirement that the government establish that the funds are directly traceable to the funds that were deposited into the foreign bank.
6. The Secretary of the Treasury or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to the account, including records maintained outside of the United States. A covered financial institution must terminate the correspondent relationship with the foreign bank if the foreign bank does not comply with the request for information.
7. Increases the maximum criminal and money penalties for money laundering from \$100,000 to \$1,000,000.
8. Allows the Secretary of the Treasury to issue regulations to ensure that concentration accounts are not used to prevent association of the identity of an individual customer with the movement of funds in the account.
9. Broadly limits a financial institution's liability to any person for submitting a suspicious activity report, for voluntarily disclosing a possible violation of law or regulation to a government agency, or for failure to provide notice of the report/disclosure to the subject of the report/disclosure.
10. Requires financial institutions to establish anti-money laundering programs that include:
 - Development of internal policies,
 - Designation of a compliance officer,
 - Ongoing employee training programs, and
 - An independent audit function.
11. Authorizes insured depository institutions to disclose in written employment references to other insured depository institutions information concerning the possible involvement of that employee in potentially unlawful activities.
12. Requires registered brokers and dealers (pursuant to rules promulgated by the Secretary of the Treasury) to file suspicious activity reports consistent with the requirements applicable to financial institutions.
13. Amends the purpose of the Bank Secrecy Act and the filing of suspicious activity reports to include protection against international terrorism.
14. Requires consumer-reporting agencies to furnish consumer reports to a government agency for the purposes of intelligence or counter-intelligence activities related to international terrorism.

15. Adds to the definition of **money transmitter** informal value transfer banking systems or networks of people facilitating the transfer of value outside of the financial institutions system. This provision attempts to establish regulatory oversight for informal “hawala” systems.

***Note:** Hawala systems consist of a transaction of liabilities, not money. That is, there is no remittance across borders. Therefore the transfer is not a capital flow because the system does not involve money/assets being transformed into other currencies. A typical scenario might be that a migrant would pay £stirling to Intermediary A (or Hawaladar A) in a community in UK (e.g. a shop owner). Hawaladar A (HA) would contact his friend, Intermediary B (Hawaladar B) in e.g. Mirpur, Pakistan. Hawaladar B (HB) then pays the migrant’s friends or family the amount in local currency.*

16. Makes it a Federal crime to operate a money transmitter business without an appropriate state license.

17. Makes the act of smuggling bulk cash in or out of the United States a criminal offense and authorizes the forfeiture of any cash or instruments of the smuggling offense.

Money Laundering Legislation and Insurance²

Although insurance companies have long been defined as financial institutions under the Bank Secrecy Act, Congress had neither defined “insurance companies” for purposes of the Bank Secrecy Act nor issued regulations regarding insurance companies. In fact, in April 2002, an anti-money laundering program requirement that would have applied to the insurance industry was deferred to allow time to study the insurance industry and to consider how anti-money laundering controls could best be applied to that industry, considering differences in size, location, and services within the industry.

In late 2005, Congress again visited the issue deciding that 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.

In establishing these programs the FATF recognized that 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.

² Federal Register, Vol 70, No 212, 11/03/05, Rules and Regulations

FATF further recognizes that not all insurance products pose a money-laundering risk. So, the requirements to develop an anti-money laundering program apply only to **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 2002 federal grand jury indictment illustrates the money laundering risks associated with insurance products and the corresponding need for vigilance in the insurance industry. That indictment charged five Colombian nationals with conspiring to launder millions of dollars originating from the illicit sale of cocaine. The scheme involved the purchase and subsequent redemption of life insurance policies. According to court documents and interviews related to that indictment, federal law enforcement officials have discovered that in recent years Colombian drug cartels bought life insurance policies in continental Europe, the United Kingdom, and in smaller jurisdictions such as the Isle of Man, to launder the proceeds of drug trafficking. Using narcotics proceeds from the United States and Mexico, the traffickers purchased 250 life insurance policies in the Isle of Man alone. The insurance policies, worth as much as \$1.9 million each, were sometimes taken out in the names of cartel associates and members of their families. The traffickers would typically cash out all or part of the Isle of Man policies prematurely, in some cases after only a year, paying penalties of 25 percent or more. The penalties, however, merely represented a “business cost” of using the insurance products to launder the illicit narcotics proceeds. Thus far, federal law enforcement officials have seized more than \$9.5 million in Florida in connection with the investigation. If the insurance companies in the relevant jurisdictions had been subject to anti-money laundering controls, they might have detected the money laundering scheme because the policyholders were authorizing unrelated third parties to withdraw money from the cash value of their policies or were frequently cashing out their policies early.

A review of the Suspicious Activity Reports (see inset box on next page) filed with the Financial Crimes Enforcement Network also 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 past 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.

The New Anti-Money Laundering Rules

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. 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.

Suspicious Activity Report

The Bank Secrecy Act of 1970 requires every financial institution to file a report of any suspicious transaction relevant to a possible violation of law or regulation. Under the law, an SAR is triggered if the dollar amount involves at least \$5000 in funds or other assets and the institution knows, suspects or has reason to suspect that the transaction involves:

- *Funds derived from illegal activity;*
- *Attempts to evade any requirements under the Bank Secrecy Act; or*
- *No apparent business or lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to be engaged in.*

The SAR should be filed with no later than 30 calendar days after the date of initial detection by the institution of facts that may form the basis for filing a SAR. If no suspect was identified on the date of the detection of the incident requiring the filing, an institution may delay their filing for an additional 30 calendar days to identify a suspect. In no case can an institution delay filing an SAR by more than 60 days after the date of initial detection of a reportable transaction. Finally, if the situation requires immediate attention, the institution is expected to notify appropriate law enforcement by telephone in addition to filing a SAR. Violations for non-compliance have been known to range as high as \$2 million!

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 new rules 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, Congress felt 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. Finally, numerous insurers already have in place compliance programs and best practices guidelines for their agents and brokers to prevent and detect fraud.

Insurance agents and brokers will play an important role in the effective operation of an insurance company's anti-money laundering program. By not placing an independent regulatory obligation on agents and brokers, Congress did not intend to minimize their role. In fact, they intend to assess the effectiveness of the rule on an ongoing basis. 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, they will consider proposing appropriate amendments to the rule. They also expect 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.

Anti-Money Laundering Training For Insurance Agents

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. In essence, it is left to the discretion of an insurance company to determine whether the training of its agents by another party is adequate. The Federal Government does **not** certify, license, or otherwise prospectively approve training programs.

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. Further exclusions for 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 were requested. Congress agreed! Some 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 anti-money laundering rules do **not include** in "covered products" reinsurance or retrocession contracts or treaties, group life insurance, or group annuities. After careful consideration of the comments, Congress also 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— they believed 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, they will reconsider this position 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, Congress emphasizes that the final rule does not require that an

insurance company adopt a company-wide, 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.

Anti-Money Laundering Plans for Insurance Companies

Section 103.137(b) of the USA Patriot Act requires that, not later than May 2, 2006, each insurance company issuing or underwriting a covered product 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.

Congress emphasized that the anti-money laundering program is only required with respect to covered products issued or underwritten by an insurance company. The anti-money laundering 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, the Financial Crimes Enforcement Network, or their designee upon request. Minimum requirements for the anti-money laundering program are set forth in section 103.137(c). Beyond these minimum requirements, however, the final rule is intended to give insurance companies the flexibility to design their programs to meet the specific risks associated with their particular business.

Minimum Requirements

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 covered products. As noted above, an insurance company's assessment of customer-related information, including methods of payment, is a key component of an effective anti-money laundering program.

Thus, an insurance company is responsible for integrating its agents and brokers into its anti- money laundering program, for obtaining relevant customer-related information from them, and for using that information to assess the money laundering risks presented by its business and to identify any "red flags" (see next page).

The specific procedures for conducting such a program are left to the **discretion** of the insurance company. Insurance companies must use the expertise that they possess about their industry and their particular lines of business to develop a program that meets the requirements of the rule. In developing a risk-based anti-money laundering program, an insurance company must consider all relevant factors affecting the risks inherent in its covered products. For example, an insurance company should consider the extent and circumstances under which its customers use cash or cash equivalents to purchase a covered product, and whether the insurance company issues or underwrites covered products to persons in a jurisdiction:

- (1) Whose government has been identified by the State Department as a sponsor of international terrorism under 22 U.S.C. 2371;
- (2) That has been designated by the Financial Action Task Force as non- cooperative with international anti- money laundering principles; 15 or

- (3) That has been found by the Secretary of the Treasury or the Director of the Financial Crimes Enforcement Network as warranting special measures due to money laundering concerns.

When assessing risks associated with particular distribution channels for its covered products, an insurance company should consider, among other things, whether an agent or broker is required to establish its own anti-money laundering program pursuant to another requirement in 31 CFR Part 103. Some have suggested, for example, excluding from an insurer's anti-money laundering program covered products sold broker dealers in securities or banks because they are already subject to an anti-money laundering program requirement.

Although Congress did not believe that a complete exclusion was appropriate, the insurance company could generally rely on the agent's own program requirements to address issues at the time of the sale if reasonable (i.e., the insurer knows of no defect in the agent's program), while the insurer's program should focus on the ongoing administration of the covered product.

Policies, procedures, and internal controls also must be reasonably designed to ensure compliance with applicable Bank Secrecy Act requirements. The only Bank Secrecy Act regulatory requirement currently applicable to insurance companies is the obligation to report on Form 8300 the receipt of cash or certain non-cash instruments totaling more than \$10,000 in one transaction or in two or more related transactions.

However, Congress also established new rules requiring insurance companies to file **Suspicious Activity Reports** (see page 14), which will apply to transactions occurring after May 2, 2006. If insurance companies become subject to additional Bank Secrecy Act requirements, their anti-money laundering programs will need to be updated accordingly. Insurance companies typically conduct their sales operations through agents. Some elements of the compliance program will be best performed by these agents, in which case it is permissible for an insurance company to make appropriate

Red Flags

Some examples of suspicious "red flags" include, but are not limited to, the following:

- The purchase of an insurance product inconsistent with the customer's needs;
- Unusual payment methods, such as cash, cash equivalents (when such a usage of cash or cash equivalents is, in fact, unusual), or structured monetary instruments;
- Early termination of a product, especially at a cost to the customer, or where payment is made by, or the refund check is directed to, an apparently unrelated third party;
- The transfer of the benefit of a product to an apparently unrelated third party;
- A customer who shows little concern for the investment performance of a product, but much concern about the early termination features of the product;
- A customer who is reluctant to provide identifying information when purchasing a product, or who provides minimal or seemingly fictitious information; and a customer who borrows the maximum amount available soon after purchasing the product.

arrangements with an agent to perform those aspects of its anti-money laundering program.

Any insurance company that arranges for its agent to perform aspects of its anti-money laundering program, however, remains responsible for the effectiveness of the program, as well as for ensuring that the appropriate examiners have access to information and records relating to the anti-money laundering program and are able to inspect the agent or the third party for purposes of the program.

Compliance

An insurance company's compliance with this regulation includes: Taking reasonable steps to identify the aspects of its operations that may give rise to applicable Bank Secrecy Act 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; and monitoring the effectiveness of its program. For example, it would not be sufficient for an insurance company simply to obtain a certification from its delegee that the company "has a satisfactory anti-money laundering program."

Compliance Officer

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, an employee or agent of an insurance company who also is a registered representative of a broker-dealer in securities or an employee of a bank would already be subject to the broker-dealer's or bank's anti-money laundering program, including its testing. In such a case, the insurance company would not have to independently test those relevant parts of the broker-dealer's or bank's program, as long as it confirms that such testing has occurred and the insurance company reviews the relevant portion of any report produced.

The person or persons should be competent and knowledgeable regarding applicable Bank Secrecy Act requirements and money laundering 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, including monitoring compliance by the company's insurance agents and insurance brokers with their obligations under the program; (2) the program is updated as necessary; and (3) appropriate persons are trained in accordance with section 103.137(c)(3). The compliance officer also should ensure that employees of the insurance company have appropriate resources to which they can address questions regarding the application of the program in light of specific facts.

AML Training

Section 103.137(c)(3) requires that an insurance company provide training for appropriate persons. Training is an integral part of any anti-money laundering program. In order for the anti-money laundering program to be effective, employees of an

insurance company with responsibility under the program must be trained in the requirements of the program and money laundering risks generally so that “red flags” associated with covered products 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 training will depend upon the functions performed. However, those persons with obligations under the anti-money laundering program must be sufficiently trained to carry out their responsibilities effectively and should receive periodic updates and refreshers regarding the anti-money laundering program.

An insurance company also must provide for the training of its insurance agents and brokers concerning their responsibilities under the company’s anti-money laundering program. An insurance company may **satisfy this requirement** by directly training its agents and brokers or by verifying that its agents and brokers have received the required training by another insurance company or by a competent third party with respect to covered products offered by the company. For purposes of the rule, a competent third party can include a third-party vendor as well as another financial institution that is subject to an anti-money laundering program requirement, such as a broker-dealer in securities or a bank.

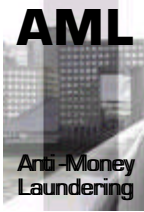
There is NO central registry for certifications of agent training. Section 103.137(c)(4) simply requires that an insurance company provide for independent testing of the program on a periodic basis to ensure that it complies with the requirements of the rule and that the program functions as designed. An outside consultant or accountant need not perform the test. A single employee of the insurance company, or a committee comprised of more than one employee, may perform the independent testing, as 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 associated with its covered products. Any recommendations resulting from such testing should be implemented promptly or submitted to senior management for consideration.

SEC Exemption May Not Qualify For Insurance Products

An insurance company that is registered (or is required to register) with the Securities and Exchange Commission as a broker-dealer in securities, to the extent such a company already is required to establish and has established an anti-money laundering program pursuant to 31 CFR 103.120, shall be deemed to be in compliance with this final rule. However, to the extent that this final rule imposes requirements with respect to activities not covered by 31 CFR 103.120 and the registered broker-dealer insurance company has adopted an anti-money laundering program that addresses only its broker-dealer activities, the company would **not be deemed in compliance** with this rule. In addition, this provision applies only to an insurance company that is itself registered or required to register with the Securities and Exchange Commission as a broker-dealer in securities, and not to a registered broker-dealer that distributes an insurance company’s products as agent.

Violations

21 E. 103.137(e)—The Financial Crimes Enforcement Network or its delegee shall examine the insurance company for compliance with this regulation, and that failure to comply may violate the Bank Secrecy Act and the final rule.



FREQUENTLY ASKED QUESTIONS REGARDING INSURANCE COMPANY ANTI-MONEY LAUNDERING REPORTING³

Note to agents: The Financial Crimes and Enforcement Network is a division of the U.S. Treasury Department developed to safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity. The following information describes questions and answers concerning their new anti-money laundering procedures required of insurance companies under the USA Patriot Act 2001 and Bank Secrecy Act of 1970. Many requirements involve the training and supervising of insurance agents and some imply that you have certain obligations and compliance issues even though you are not specifically directed. We feel this is important reading in order to fully understand the new rules and law.

1. Why is the Financial Crimes Enforcement Network issuing a regulation requiring insurance companies to establish anti-money laundering programs?

As with all regulations requiring the establishment of an anti-money laundering program, this regulation is passed to better protect a class of financial institutions – in this case, the insurance industry – from potential abuse by criminals and terrorists, thereby enhancing the protection of the U.S. financial system generally. The characteristics of financial products, including certain insurance products, make them potentially vulnerable to those seeking to launder money. This regulation is a key step in ensuring that the Bank Secrecy Act is applied appropriately to these businesses.

Recognizing the need for a more comprehensive anti-money laundering regime, Congress passed and the President signed into law the USA PATRIOT Act, which, among other things, requires that all entities defined as financial institutions for Bank Secrecy Act purposes establish anti-money laundering programs. An insurance company is defined as a “financial institution” under the Bank Secrecy Act. The USA PATRIOT Act further directs the Secretary of the Treasury to prescribe through regulation minimum standards for such programs.

2. Does the final rule apply to all insurance companies?

No. The term “insurance company” or “insurer” is defined in the final rule to describe any person engaged within the United States as a business in the issuing or underwriting of “covered products.” Covered products, discussed further below, are those insurance products that we have determined to present a higher degree of risk for money laundering. The phrase “as a business” in the definition of “insurance company” is intended to exclude those persons that offer annuities or other covered products as an incidental part of their business. For example, a tax-exempt organization that offers charitable gift annuities, as defined in section 501(m)(5) of the Internal Revenue Code, that would not otherwise fall within the definition of an insurance company, would not be considered an insurance company for purposes of the final rule. If an insurance company that is not presently issuing or underwriting a covered product should do so in

³ Department of Treasury, Financial Crimes Enforcement Network Bulletin

the future, the insurance company would then become subject to the rule (but only to the extent of its business relating to covered products). Conversely, if an insurance company ceases issuing or underwriting covered products, the insurance company would no longer be subject to the rule. An insurance company that is registered with the Securities and Exchange Commission as a broker-dealer in securities would not be required to establish a duplicate program under the final rule for insurance companies. Broker-dealers in securities currently are subject to an independent anti-money laundering program obligation under our regulations, CFR 103.120; therefore, the insurance company would not be required to establish a separate anti-money laundering program in order to comply with the final rule, as long as it has established an anti-money laundering program pursuant to that requirement and complies with the program.¹ However, the company should evaluate the extent (if any) to which its existing anti-money laundering program should be revised to appropriately address the risks of doing business in covered insurance products.

3. What are “covered products”?

For purposes of the final insurance company rule, the term “covered product” is defined to mean:

A ***permanent life insurance policy***, other than a group life insurance policy; An ***annuity contract***, other than a group annuity contract; and ***Any other insurance product with cash value or investment features***. The definition incorporates a functional approach, and encompasses any insurance product having the same kinds of features that make permanent life insurance and annuity products more at risk of being used for money laundering, e.g., having a cash value or investment feature. To the extent that term life insurance, property and casualty insurance, health insurance, and other kinds of insurance do not exhibit these features, they are not products covered by the rule.

4. Which insurance products are not “covered products” pursuant to the rule?

Because they pose a lower risk for money laundering, the following products are not defined as “covered products” in the final rule:

- Group insurance products
- Products offered by charitable organizations, e.g. charitable annuities
- Term (including credit) life, property, casualty, health, or title insurance
- Reinsurance and retrocession contracts.

Contracts of indemnity and structured settlements (including workers’ compensation payments) are not within the definition of “covered products” for purposes of the final rule.

5. Does the final rule require insurance agents and brokers to establish anti money laundering programs?

Insurance agents and brokers are not required by the final rule to have separate anti-money laundering programs. However, insurance agents and brokers are an integral part of the insurance industry due to their contact with customers. Insurance agents and

brokers typically are involved in sales operations and are therefore in direct contact with customers. As a result, 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.

6. What are the requirements for an anti-money laundering program?

The final rule requires an insurance company that issues or underwrites covered products to develop and implement a written anti-money laundering program applicable to its covered products that is reasonably designed to prevent the insurance company from being used to facilitate money laundering. The program must be approved by senior management and made available to the Department of the Treasury (or its delegate) upon request.

As is true of all of our anti-money laundering program rules, insurance companies must develop a risk-based program. Under the Bank Secrecy Act, financial institutions are required to identify, assess, and mitigate the risk that their business will be abused by criminals. Risks can be jurisdictional, product-related, service-related, or client-related. Regardless of where those risks arise, financial institutions covered by our regulations must take reasonable steps to mitigate them. Compliance is risk-based, meaning that a financial institution must devote more compliance resources to the areas of its business that pose the greatest risk. Moreover, as is true for all industries we regulate, we do not expect businesses of different sizes and circumstances to have the same types of anti money laundering programs.

We believe effective implementation must be predicated upon your knowledge of your business, a careful assessment of the vulnerabilities of your business to money laundering, and adoption of controls appropriate to that risk. At a minimum, insurance companies must establish an anti-money laundering program that comprises the four elements set forth below. Our website (www.fincen.gov) contains information and updates on money laundering and terrorist financing risks as they apply to the insurance industry. We do not expect that this program can prevent all potential money laundering.

What *is* expected is that your business will take prudent steps, with the same kind of thought and care that you take to guard against other crimes, such as theft or fraud. It should be noted that the required components are minimum requirements. Insurance companies that offer a diversity of insurance products may decide to adopt institution-

wide anti-money laundering programs regardless of the types of products offered. However, the final rule requirement applies only to covered products offered by the company.

(1) A compliance officer who is responsible for ensuring that the program is implemented effectively.

The compliance officer is an employee or group of employees who will be responsible for the day-to-day operation of your anti-money laundering program. In particular, this person (or persons) will be responsible for ensuring that the steps within your own program are fully implemented. As such, this person should be someone with enough authority to achieve this important task. The amount of time devoted to these duties will depend on the level of risk. An insurance company is not required to designate a person to serve on a full-time basis as a compliance officer for purposes of the final rule unless the level of risk or volume of transactions warrants. If your business faces a very high level of risk for money laundering, then a great deal will be required of this person. If your exposure to these risks is more moderate, then the level of effort will be commensurate with that risk.

In all cases, however, the compliance officer should be thoroughly familiar with the operations of the business itself and with all aspects of your anti-money laundering program, as well as with the requirements of the Bank Secrecy Act and applicable Financial Crimes Enforcement Network forms, and should have read carefully all applicable documents we issue or post on our web page (www.fincen.gov).

(2) Policies, procedures, and internal controls.

Policies, procedures, and internal controls must be developed, based on the insurance company's assessment of the money laundering risk associated with its business, that are reasonably designed to enable the insurance company to comply with the applicable requirements of the Bank Secrecy Act and to prevent the insurance company from being used by money launderers.

As the preamble to the rule describes, you should assess the extent to which your particular business is susceptible to money laundering. Those companies dealing with covered products that pose a significantly higher risk require greater diligence for detecting transactions that may involve money laundering. Using customer and other information obtained through agents, brokers or otherwise, an insurance company can assess the money laundering risks presented by its business based on such factors as the particular types and locations of customers served, distribution channels, and products offered.

(3) Ongoing training of appropriate persons concerning their responsibilities under the program.

You should first consider what training is appropriate for each individual employee. Some employees may require no training on the program, given their particular duties. Others may require a great deal of training. The training should be clearly understood by your employees, agents, brokers, and others doing business with covered products. The compliance officer should be available to answer all questions posed by employees.

Remember that you should periodically retrain your employees on your program to ensure that they understand and can fully implement your program.

(4) Independent testing to monitor and maintain an adequate program.

Some person or group of people who are not working specifically for the compliance officer on the compliance program should be selected to determine whether the program complies with the requirements of the rule and that the program functions as designed. For example, if the program requires that a particular employee be trained once every six months, then the independent testing should determine whether the training occurred and whether the training was adequate. Independent testing does not mean that an outside party must be hired, although outside parties may be utilized to conduct the independent review. It does mean, though, that the testing should be a fair and unbiased appraisal of the success in implementing the anti-money laundering program, and the results of the independent testing should be put into writing, including any recommendations to senior management.

Independent testers should carefully consider all of the decisions made by the compliance officer, such as the determination of the level of risk faced by the insurance company for money laundering, the frequency of training, etc. The independent testing is intended to confirm that the program complies with the requirements of the rule and that the program functions as designed.

7. Is an insurance company required to train all of its employees in-house? What about training of brokers and agents?

An insurance company may satisfy the training requirement under its anti-money laundering program with respect to its employees, agents and brokers by directly training such persons or by verifying that those employees, agents and brokers have received adequate training by another insurance company or by a competent third party with respect to the covered products offered by the insurance company. For purposes of the rule, a competent third party can include, among others, another financial institution that is subject to an anti-money laundering program, such as a broker-dealer in securities or a bank.

An insurance company remains responsible for assuring compliance with the final rule and monitoring the effectiveness of its training program. The nature of the insurance company's review of a training program performed by another entity depends upon the facts and circumstances of the particular situation. For example, if the training is performed by another entity that has its own anti-money laundering program (such as a broker-dealer or bank), the insurance company's evaluation of the training program may be less stringent than if a third-party contractor performs the training. Mere certification of attendance at a program is insufficient; rather, evaluation of the substance of the training is essential.

8. What resources are available to help an insurance company to establish an adequate program?

The preambles to the final rules and these Frequently Asked Questions provide the foundation for the process of establishing an anti-money laundering program. Going forward, we will be issuing additional guidance to the industry. All such guidance will be

posted on our website (www.fincen.gov). Additionally, we operate a Regulatory Helpline (1-800-949-2732), to provide answers to specific regulatory or compliance questions.

9. When must we implement our Anti-Money Laundering Program?

You will have 180 days from when the final rule is published in the *Federal Register* to implement your anti-money laundering program -- i.e., May 2, 2006.

10. Should insurance companies continue to file Form 8300 – Report of Cash Payments Over \$10,000 Received in a Trade or Business?

Yes. Insurance companies should continue to file Form 8300 in appropriate situations to report the receipt of cash over \$10,000. There is no requirement at this time for insurance companies to file Currency Transaction Reports. Also, Form 8300 includes Box 1b for reporting of suspicious transactions.

Because covered insurance companies will be required to file Suspicious Activity Reports (see below) as part of their anti-money laundering program, the proposed Suspicious Activity Report for Insurance Companies form will be the required medium for reporting suspicious activity. An insurance company is not precluded from also checking the “suspicious transaction” box, as appropriate, when filing a Form 8300; however, checking the box on the Form 8300 is not required, and in any event will *not* satisfy the insurance company’s obligation to file a Suspicious Activity Report in the appropriate circumstances.

11. Are insurance companies required to file Suspicious Activity Reports as a part of their anti-money laundering programs?

Yes. Pursuant to a final rule adopted at the same time as the anti-money laundering program final rule, insurance companies will now be required to file Suspicious Activity Reports. This requirement will take effect 180 days from when the final rule is published in the *Federal Register*.

We have proposed a new suspicious activity reporting form for insurance companies (FinCEN Form 108 – Suspicious Activity Report by Insurance Companies). Until such time as that form has been adopted and is available for use, insurance companies should use FinCEN Form 101 – Suspicious Activity Report by Securities and Futures Industries to report suspicious transactions. Importantly, to assist law enforcement in locating reports filed by insurance companies, the words “Insurance SAR” should be entered on the first line of the Narrative. Under the final rule requiring suspicious activity reporting by insurance companies, covered insurance companies must file Suspicious Activity Reports to report suspicious transactions, rather than checking the “suspicious transaction” box on Form 8300 (Box 1b) (see above). It may be appropriate for an insurance company to file a

Form 8300 for receipt of cash and other items over \$10,000 as well as to file a Suspicious Activity Report when the circumstances surrounding the receipt of cash and other items are suspicious.

12. What are examples of suspicious activities with regard to insurance products?

Some examples of "red flags" include, but are not limited to, the following: the purchase of an insurance product inconsistent with the customer's needs; unusual payment methods, such as cash, cash equivalents (when such a usage of cash or cash equivalents is, in fact, unusual), or structured monetary instruments; early termination of a product (including during the "free look" period), especially at a cost to the customer, or where payment is made by, or the refund check is directed to, an apparently unrelated third party; the transfer of the benefit of a product to an apparently unrelated third party; a customer who shows little concern for the investment performance of a product, but a great deal of concern about the early termination features of the product; a customer who is reluctant to provide identifying information when purchasing a product, or who provides minimal or seemingly fictitious information; and a customer who borrows the maximum amount available soon after purchasing the product.

13. How should suspicious activity involving variable insurance products funded by separate accounts that meet definition of a "mutual fund" be reported?

Some insurance companies issue variable insurance products funded by separate accounts, some of which meet the definition of a mutual fund. We are in the process of finalizing a rule that would require mutual funds to themselves file suspicious activity reports. When that final rule becomes effective, we will amend the insurance company suspicious activity reporting rule to ensure that such suspicious activity is reported under the mutual fund rule.

Until such time as a final rule requiring suspicious activity reporting by mutual funds is adopted, however, insurance companies that issue variable insurance products funded by separate accounts that meet the definition of a mutual fund may report suspicious activity on FinCEN Form 101 – Suspicious Activity Report by Securities and Futures Industries.

14. Are insurance brokers and agents required to file suspicious activity reports?

The ***obligation to identify*** and report suspicious transactions applies only to an insurance company, and not to its agents or brokers. 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 an insurance company to establish and implement policies and procedures reasonably designed to obtain customer-related information necessary to detect suspicious activity from all relevant sources, including from its agents and brokers, and to report suspicious activity based on such information.

The final rule imposes a direct obligation only on insurance companies, and not on their agents or brokers, for a number of reasons. First, whether an insurance company sells its products directly or through agents, we believe 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 illegally derived funds. Second, insurance companies, due to their much larger size relative to that of their numerous agents and brokers, are in a much better position to shoulder the costs of compliance connected with the sale of their products. Finally, numerous insurers already have in place compliance programs and best practices guidelines for their agents and brokers to prevent and detect fraud. We believe that insurance companies

largely will be able to integrate their obligation to report suspicious transactions 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 obligation to report suspicious transactions. By not placing an independent reporting obligation on agents and brokers, we do not intend to minimize their role. We intend to assess the effectiveness of the rule on an ongoing basis. 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, we will consider proposing appropriate amendments to the rule. We also expect that an insurance company, when faced with a non-compliant agent or broker, will take necessary actions to secure such compliance, including, when appropriate, terminating its business relationship with such an agent or broker.

Certain insurance agents and insurance brokers may be broker-dealers in securities with an independent obligation to report suspicious activity under another Bank Secrecy Act regulation.

15. Are joint Suspicious Activity Report filings permissible?

Yes. In circumstances where two or more financial institutions subject to suspicious activity reporting requirements under the Bank Secrecy Act are involved in a common or related transaction, and each financial institution has information about the transaction, a joint Suspicious Activity Report may be filed. Neither the Bank Secrecy Act nor regulations promulgated by us prohibit financial institutions from sharing information relating to suspicious activities as long as no persons involved in the transaction are notified.

An insurance company must keep a copy of the filed Suspicious Activity Report form for its records. The Suspicious Activity Report and the original or business record equivalent of any supporting documentation must be maintained in the insurance company's records for a period of five years from the date of filing. An insurance company must also retain copies of reports (and supporting documentation) provided to it by its agents that are required to make reports by another provision in 31 CFR Part 103 when the agents and the company file a joint report regarding a transaction involving both companies.

A joint Suspicious Activity Report that is filed with us in the manner described above will be deemed to have been filed by each financial institution involved in the underlying transaction, thereby satisfying each financial institution's obligation to report suspicious activity. Financial institutions may share information pertaining to the transaction, as long as no persons involved in the transaction are notified. Such communications between financial institutions for the purpose of filing or determining whether to file a joint Suspicious Activity Report are protected by a safe harbor from civil liability pursuant to 31 U.S.C. 5318(g), as disclosures authorized under that section's implementing regulations and interpretative guidance.

In all such joint filings, only one of the filing institutions should be identified as the "filer" in the filer identification section of the form (unless the form accommodates multiple filers, as the Suspicious Activity Report for Insurance Companies will do). The Narrative section of the suspicious activity report must include the words "joint filing" and must identify the other financial institution or institutions on whose behalf the report is being

filed (unless the form will accommodate multiple filers, in which case there is no need to include that information in the Narrative section).

16. If an insurance company files a Suspicious Activity Report voluntarily, will it be protected from civil liability?

Yes. Pursuant to 31 U.S.C. 5318(g)(3): “Any financial institution that makes a voluntary disclosure of any possible violation of law or regulation to a government agency ...shall not be liable to any person under any law or regulation of the United States... or regulation of any State...for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure.”

It is the intent of this provision of the Bank Secrecy Act to provide the greatest possible protection to financial institutions, in the form of a “safe harbor,” to encourage the filing of Suspicious Activity Reports if appropriate.

17. May we disclose that a Suspicious Activity report was filed? What if we receive a civil subpoena?

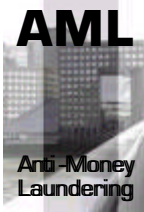
There are statutory and regulatory prohibitions against the disclosure of information filed in, or the fact of filing, a Suspicious Activity Report whether the report is required or is filed voluntarily. Thus, insurance companies filing the proposed Suspicious Activity Report by Insurance Companies (or receiving a copy of filed joint Suspicious Activity Reports from another financial institution involved in the same transaction) are specifically prohibited from disclosing that a Suspicious Activity Report has been filed or the information contained therein, except to appropriate law enforcement and regulatory agencies.

If you are served with any subpoena requiring disclosure of the fact that a Suspicious Activity Report has been filed or of a copy of the Suspicious Activity Report itself, except to the extent that the subpoena is submitted by an appropriate law enforcement or supervisory agency, you should neither confirm nor deny the existence of the Suspicious Activity Report. You also should immediately notify the Office of Chief Counsel at the Financial Crimes Enforcement Network (703-905-3590).

18. Certain financial institutions participate in information sharing pursuant to section 314(b) of the USA PATRIOT Act and Financial Crimes Enforcement Network regulations at 31 CFR 103.110. May insurance companies now participate in that information sharing?

Yes. Pursuant to 31 CFR 103.110(a)(2), information sharing between financial institutions concerning terrorist financing and/or money laundering is available to financial institutions that have an obligation to establish anti-money laundering programs.

Once an insurance company subject to the insurance company anti-money laundering program rule has established its anti-money laundering program it may file a certification for purposes of section 314(b) of the USA PATRIOT Act and 31 CFR 103.110.



ANTI-MONEY LAUNDERING CONTROLS AND PROCEDURES

Insurers and agents should be constantly vigilant in deterring criminals from making use of them for the purposes of money laundering or the financing of terrorism. By understanding the risks of money laundering and the financing of terrorism, insurers are in a position to determine what can be done to control these risks, and which procedures and measures can be implemented effectively and efficiently.

For reasons of sound business practice and proper risk management you and your insurer should already have controls in place to assess the risk of each business relationships. As customer due diligence is a business practice suitable not just for commercial risk assessment and fraud prevention, but also to prevent money laundering and the financing of terrorism, control measures should be linked to these existing controls. The concept of customer due diligence goes beyond the identification and verification of only the policyholder – it extends to identification of the potential risks of the whole business relationship.

The duty of vigilance consists mainly of the following elements:

- Customer due diligence, including underwriting checks and verification of identity
- Recognition and reporting of suspicious customers/transactions, and
- Provisions affecting the organization and the staff of the insurer, such as a compliance and audit environment, keeping of records, the recruitment of staff and training.

Customer Due Diligence

Insurers should ***know the customers*** with whom they are dealing. A first step in setting up a system of customer due diligence is to develop clear, written and risk based client acceptance policies and procedures, which among other things concern the types of products offered in combination with different client profiles. These policies and procedures should be built on the strategic policies of the board of directors of the insurer, including policies on products, markets and clients.

The insurer's strategic policies will determine its exposure to risks such as underwriting risk, reputational risk, operational risk, concentration risk¹⁰ and legal risk. After determining the strategic policies, client acceptance policies should be established, taking account of risk factors such as the background and geographical base of the customer and/or beneficial owner and the complexity of the business relationship for other factors). This is why – as indicated above – control measures and procedures with respect to anti-money laundering should be an integral part of the overall customer due diligence.

Insurers should be aware that, for example, they are more vulnerable to money laundering if they sell short-term coverage by means of a single premium policy than if they sell group pensions to an employer with annuities to be paid after retirement. The former is more sensitive to money laundering and therefore calls for more intensive checks on the background of the client and the origin of the premium than the latter.

Customer **due diligence measures** that should be taken by insurers, assisted by agents, include:

- Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information
- Determining whether the customer is acting on behalf of another person, and then taking reasonable steps to obtain sufficient identification data to verify the identity of that other person
- Identifying the (ultimate) beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the insurer is satisfied that it knows who the beneficial owner is. For legal persons and arrangements insurers should take reasonable measures to understand the ownership and control structure of the customer
- Obtaining information on the purpose and intended nature of the business relationship and other relevant factors
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the insurer's knowledge of the customer and/or beneficial owner, their business and risk profile, including, where necessary, the source of funds.

The extent and specific form of these measures may be determined following a risk analysis based upon relevant factors including the customer, the business relationship and the transaction(s). Enhanced due diligence is called for with respect to higher risk categories.

Decisions taken on establishing relationships with higher risk customers and/or beneficial owners should be taken by senior management. Subject to national legal requirements insurers may apply reduced or simplified measures in the case of low risk categories.

Prior to the establishment of a business relationship, the insurer should assess the characteristics of the required product, the purpose and nature of the business relationship and any other relevant factors in order to create and maintain a risk profile of the customer relationship. Based on this assessment, the insurer should decide whether or not to accept the business relationship. As a matter of principle, insurers should not offer insurance to customers or for beneficiaries that obviously use fictitious names or whose identity is kept anonymous.

Factors to consider when creating a **risk profile**, which are not set out in any particular order of importance and which should not be considered exhaustive, include (where appropriate):

- Type and background of customer and/or beneficial owner
- The customer's and/or beneficial owner's geographical base
- The geographical sphere of the activities of the customer and/or beneficial owner
- The nature of the activities
- The means of payment as well as the type of payment (cash, wire transfer, other means of payment)

- The source of funds
- The source of wealth
- The frequency and scale of activity
- The type and complexity of the business relationship
- Whether or not payments will be made to third parties
- Whether a business relationship is dormant
- Any bearer arrangements
- Suspicion or knowledge of money laundering, financing of terrorism or other crime.
- Customer indifference to surrender charges or penalties

The requirements for customer due diligence should apply to all new customers as well as –on the basis of materiality and risk –to existing customers and/or beneficial owners. As to the latter the insurer should conduct due diligence at appropriate times. In insurance, various transactions or ‘trigger events’ occur after the contract date and indicate where due diligence may be applicable. These trigger events include claims notification, surrender requests and policy alterations, including changes in beneficiaries.

The requirement for an insurer to pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose is essential to both the establishment of a business relationship and to ongoing due diligence. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.¹⁴ In this respect “transactions” should be interpreted in a broad sense, meaning inquiries and applications for an insurance policy, premium payments, requests for changes in benefits, beneficiaries, duration, etc.

In the event of failure to complete verification of any relevant verification subject or to obtain information on the purpose and intended nature of the business relationship, the insurer should not conclude the insurance contract, perform the transaction, or should terminate the business relationship. The insurer should also consider making a Suspicious Activity Report.

Establishing A Business Relationship

Before an insurance contract is concluded between customer and insurer there is already a pre-contractual business relationship between these two and possibly other parties. After a policy is taken out:

- The insurer covers a certain risk described in the contract and policy conditions
- Certain transactions may take place such as premium payments, payments of advance or final benefits, and
- Certain events may occur such as a change in cover or a change of beneficiaries.

The insurer will need to carefully assess the specific background, and other conditions and needs of the customer. This assessment is already being carried out for commercial purposes (determining the risk exposure of the insurer and setting an adequate premium) as well as for reasons of active client management. To achieve this, the insurer will collect relevant information, for example details of source of funds, income,

employment, family situation, medical history, etc. This will lead to a customer profile which could serve as a reference to establish the purpose of the contract and to monitor subsequent transactions and events.

The insurer should realize that creating a customer profile is also of importance for anti-money laundering purposes and therefore for the protection of the integrity of the insurer and its business.

In addition, the beneficial owner should also be identified and verified. For the purposes of this guidance paper the expression beneficial owner applies to the owner/controller of the policyholder as well as to the beneficiary to the contract.

With regard to reinsurance, due to the nature of the business and the lack of a contractual relationship between the policyholder and the reinsurance company, it is often impractical or impossible for the reinsurer to carry out verification of the policyholder or the beneficial owner. Therefore, for reinsurance business reinsurers should only deal with ceding insurers (1) that are licensed or otherwise authorised to issue insurance policies and (2) which have warranted or otherwise confirmed that they apply AML/CFT standards at least equivalent to those in this guidance paper, provided there is no information available to the contrary for instance from FATF and trade associations or from the reinsurers' visits to the premises of the insurer.

When the identity of customers and beneficial owners with respect to the insurance contract has been established the insurer is able to assess the risk to its business by checking customers and beneficial owners against internal and external information on known fraudsters or money launderers (possibly available from industry databases) and on known or suspected terrorists (publicly available on sanctions lists such as those published by the United Nations). Otherwise insurers are encouraged to use all available sources of information when considering whether or not to accept a risk. Identification and subsequent verification will also prevent anonymity of policyholders or beneficiaries and the use of fictitious names.

Timing Of Identification and Verification

Ideally, ***identification and verification*** of customers and beneficial owners should take place when the business relationship with that person is ***established***. This means that (the owner / controller of) the policyholder needs to be identified and their identity verified before, or at the moment when, the insurance contract is concluded. Valid exceptions are mentioned in the following paragraphs.

Identification and verification of the beneficiary may take place after the insurance contract has been concluded with the policyholder, provided the money laundering risks and financing of terrorism risks are effectively managed. However, identification and verification should occur at or before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

Where a policyholder and/or beneficiary is permitted to utilise the business relationship prior to verification, financial institutions should be required to adopt risk management procedures concerning the conditions under which this may occur. These procedures should include measures such as a limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions

being carried out outside the expected norms for that type of relationship. Where the insurer has already commenced the business relationship and is unable to comply with the verification requirements it should terminate the business relationship and consider making a suspicious transaction report.

Examples of situations where a business relationship could be used prior to verification are:

- Group pension schemes
- Non-face-to-face customers
- Premium payment made before the application has been processed and the risk accepted, and
- Using a policy as collateral.

In addition, in the case of non-face-to-face business verification may be allowed after establishing the business relationship. However, insurers must have policies and procedures in place to address the specific risks associated with non-face-to-face business relationships and transactions.

Example Transactions Events In The Course of The Business Relationship

The insurer should perform ongoing due diligence on the business relationship. In general the insurer should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. It should assess if the change/transaction does not fit the profile of the customer and/or beneficial owner or is for some other reason unusual or suspicious. Enhanced due diligence is required with respect to higher risk categories. The CDD program should be established in such a way that the insurer is able to adequately gather and analyze information.

Examples of ***transactions or trigger events*** after establishment of the contract that ***require attention*** include, but are not limited to:

- A change in beneficiaries (for instance, to include non-family members, or a request for payments to be made to persons other than beneficiaries)
- A change/increase of insured capital and/or of the premium payment (for instance, which appear unusual in the light of the policyholder's income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party)
- Use of cash and/or payment of large single premiums
- Payment/surrender by a wire transfer from/to foreign parties
- Payment by banking instruments which allow anonymity of the transaction
- Change of address and/or place of residence of the policyholder, in particular, tax residence
- Lump sum top-ups to an existing life insurance contract
- Lump sum contributions to personal pension contracts
- Requests for prepayment of benefits
- Use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a

reputable financial institution) change of the type of benefit (for instance, change of type of payment from an annuity to a lump sum payment)

- Early surrender of the policy or change of the duration (where this causes penalties or loss of tax relief)
- Request for payment of benefits at the maturity date.

The above list is not exhaustive. Insurers should consider other types of transactions or trigger events which are appropriate to their type of business.

Occurrence of these transactions and events does not imply that (full) customer due diligence needs to be applied. If identification and verification have already been performed, the insurer is entitled to rely on this unless doubts arise about the veracity of that information it holds. As an example, doubts might arise if benefits from one policy of insurance are used to fund the premium payments of another policy of insurance.

Methods of Identification and Verification

This course does not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. It does set out what, as a matter of good practice, may reasonably be expected of insurers. Since, however, this guidance paper is neither mandatory nor exhaustive, there may be cases where an insurer has properly satisfied itself that verification has been achieved by other means which it can justify to the appropriate authorities as reasonable in the circumstances.

The best possible identification documentation should be obtained from each verification subject. "Best possible" means that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

Individuals

The following personal information should be considered:

- Full name(s) used
- Date and place of birth
- Nationality
- Current permanent address including zip code
- Occupation and name of employer (if self-employed, the nature of the self-employment), and
- Specimen signature of the individual.

Original documents should be signed by the individual and if the individual is met face to-face, the documents should preferably bear a photograph of the individual. Where copies of documents are provided, appropriate authorities and professionals may certify the authenticity of the copies.

Documents which are easily obtained in any name should not be accepted uncritically. These documents include birth certificates, an identity card issued by the employer of the applicant even if bearing a photograph, credit cards, business cards, driving licences (not bearing a photograph), provisional driving licenses and student union cards.

Legal persons, companies, partnerships and other institutions/arrangements

The types of measures normally needed to perform CDD on legal persons, companies, partnerships and other institutions/arrangements satisfactorily require identification of the natural persons with a controlling interest and the natural persons who comprise the mind and management of the legal person or arrangement. Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, it is not necessary to identify and verify the identity of any shareholder of that company.

Where customers and/or beneficial owners are ***legal persons or legal arrangements***, the insurers should:

- Verify that any person purporting to act on behalf of the customer and/or beneficial owner is so authorized and identify and verify the identity of that person or business
- Verify the legal status of the legal person or legal arrangement, e.g. by obtaining proof of incorporation or similar evidence of establishment or existence, and
- Form an understanding of the ownership and control structure of the customer and/or beneficial owner.

Where trusts or similar arrangements are used, particular care should be taken in understanding the substance and form of the entity. Where the customer is a trust, the insurer should verify the identity of the trustees, any other person exercising effective control over the trust property, the settlors and the beneficiaries. Should it not be possible to verify the identity of the beneficiaries when the policy is taken out, verification must be carried out prior to any payments being made.

When dealing with the identification and verification of companies, trust and other legal entities the insurer should be aware of vehicles, corporate or otherwise, that are known to be misused for illicit purposes.

Sufficient verification should be undertaken to ensure that the individuals purporting to act on behalf of an entity are authorized to do so.

The following documents or their equivalent should be considered:

- Certificate of incorporation
- The name(s) and address(es) of the beneficial owner(s) and/or the person(s) on whose instructions the signatories of the customer are empowered to act
- Constitutional documents e.g. memorandum and articles of association, partnership agreements
- Copies of powers of attorney or other authorities given by the entity.

In all transactions undertaken on behalf of an employer-sponsored pension or savings scheme the insurer should, at a minimum, undertake verification of the principal employer and the trustees of the scheme (if any).

Verification of the principal employer should be conducted by the insurer in accordance with the procedures for verification of institutional applicants for business.

Verification of any trustees of the scheme will generally consist of an inspection of the relevant documentation, which may include:

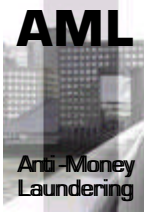
- The trust deed and/or instrument and any supplementary documentation
- A memorandum of the names and addresses of current trustees (if any)
- Extracts from public registers
- References from professional advisers or investment managers.

As legal controls vary between jurisdictions, particular attention may need to be given to the place of origin of such documentation and the background against which it is produced.

New or developing technologies

New or developing technologies can be used to market insurance products. **E-commerce** or sales through the internet is an example of this. Although for this type face-to-face business verification may be allowed after establishing the business relationship, the insurer should nevertheless complete verification.

Although a non-face-to-face customer can produce the same documentation as a face to face customer, it is **more difficult to verify their identity**. Therefore, in accepting business from non-face-to-face customers an insurer should use equally effective identification procedures as those available for face-to-face customer acceptance, supplemented with specific and adequate measures to mitigate the higher risk.



INDICATORS AND EXAMPLES OF INSURANCE MONEY LAUNDERING SCHEMES

The following examples are possible indicators of a suspicious transaction and may give cause for an agent to alert his insurer to file a Suspicious Activity Report:

- Application for a policy from a potential client in a distant place where a comparable policy could be provided “closer to home”
- Application for business outside the policyholder’s normal pattern of business
- Introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organized criminal activities (e.g. drug trafficking or terrorist activity) or corruption are prevalent
- Any want of information or delay in the provision of information to enable verification to be completed
- An atypical incidence of pre-payment of insurance premiums
- The client accepts very unfavorable conditions unrelated to his or her health or age
- The transaction involves use and payment of a performance bond resulting in a cross border payment (wire transfers) = the first (or single) premium is paid from a bank account outside the country
- Large fund flows through non-resident accounts with brokerage firms
- Insurance policies with premiums that exceed the client’s apparent means
- The client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment
- Insurance policies with values that appear to be inconsistent with the client’s insurance needs
- The client conducts a transaction that results in a conspicuous increase of investment contributions
- Any transaction involving an undisclosed party
- Early termination of a product, especially at a loss, or where cash was tendered and/or the refund check is to a third party
- A transfer of the benefit of a product to an apparently unrelated third party
- A change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy)
- Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder
- Requests for a large purchase of a lump sum contract where the policyholder has usually made small, regular payments
- Attempts to use a third party check to make a proposed purchase of a policy
- The applicant for insurance business shows no concern for the performance of the policy but much interest in the early cancellation of the contract
- The applicant for insurance business attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by checks or other payment instruments

- The applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency
- The applicant for insurance business is reluctant to provide normal information when applying for a policy, providing minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify
- The applicant for insurance business appears to have policies with several institutions
- The applicant for insurance business purchases policies in amounts considered beyond the customer's apparent means
- The applicant for insurance business establishes a large insurance policy and within a short time period cancels the policy, requests the return of the cash value payable to a third party
- The applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy
- The applicant for insurance business use a mailing address outside the insurance supervisor's jurisdiction and where during the verification process it is discovered that the home telephone has been disconnected.

Life insurance

- A company director from Company W, Mr. H, set up a money laundering scheme involving two companies, each one established under two different legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director. These companies wired the sum of \$1.1 million to the accounts of Mr. H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr. H also received transfers from Country C. Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers, the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some \$1.2 million and represented the last step in the laundering operation.
- An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the assured.
- On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank *accounts* and then transferred to an *account* in another jurisdiction. The drug trafficker then entered into a \$75,000 life insurance policy. Payment for the policy was made by two separate wire transfers from the overseas *accounts*. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer had received instructions for the early surrender of the policy.

- In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over \$1.5 million was initially placed with a bank in England. The “layering process” involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent’s supervisor was also charged with violating the money laundering statute. This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.
- Customs officials in Country X initiated an investigation which identified a narcotics trafficking organization utilized the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries identified narcotic traffickers were laundering funds through Insurance firm Z located in an off-shore jurisdiction. Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an insurance company and the funds were apparently clean. To date, this investigation has identified that over \$29 million was laundered through this scheme, of which over \$9 million dollars has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and Country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities involved individuals associated with Insurance firm Z.
- A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around \$400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual’s fraudulent management activity.
- A life insurer learned from the media that a foreigner, with whom it had two life-insurance contracts, was involved in Mafia activities in his/her country. The contracts were of 33 years duration. One provided for a payment of close to the equivalent of \$1 million in case of death. The other was a mixed insurance with value of over half this amount.
- A client domiciled in a country party to a treaty on the freedom of cross-border provision of insurance services, contracted with a life insurer for a foreign life insurance for 5 years with death cover for a down payment equivalent to around \$7 million. The beneficiary was altered twice: 3 months after the establishment of the policy and 2 months before the expiry of the insurance. The insured remained the same. The insurer reported the case.

Non-Life Insurance

- A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and suborned the

intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. In this way, the money launderer was able to receive claims checks which could be used to launder funds. The funds appeared to come from a reputable insurance company, and few questioned the source of the funds having seen the name of the company on the check or wire transfer.

- Four agencies were forced to freeze funds after US court action that followed an investigation into Latin American drugs smuggling. The drug trafficking investigation, code named Golden Jet, was coordinated by the Drug Enforcement Agency (DEA) based in the USA but also involved the FBI and the UK authorities. The funds frozen by the court action related to insurance money deposited at insurance brokers for around 50 aircraft. It is understood that the brokers affected by the court order included some of the largest UK insurance brokers. The case highlighted the potential vulnerability of the insurance market to sophisticated and large scale drug trafficking and money laundering operators. The court order froze aircraft insurance premiums taken out by 17 Colombian and Panamanian air cargo companies and by 9 individuals. The action named 50 aircraft, including 13 Boeing 727s, 1 Boeing 707, 1 French Caravelle and 2 Hercules C130 transport aircraft. The British end of the action was just one small part of a massive anti-drug trafficking action co-ordinated by the DEA. Officials of the DEA believe Golden Jet is one of the biggest blows they have been able to strike against the narcotics trade. The American authorities led by the DEA swooped on an alleged Colombian drugs baron and tons of cocaine valued at many billions of dollars were seized and a massive cocaine processing factory located in Colombia together with aircraft valued at more than \$22 million were destroyed in the DEA coordinated action. According to the indictment, the cargo companies were responsible for shipping tons of cocaine from South to North America all through the 1980s and early 1990s, providing a link between the producers and the consumers of the drugs. Much of the cocaine flowing into the USA was transported into the country by air. During this period the Colombian cartels rose to wealth and prominence, aided by those transport links.

Intermediaries

- A person (later arrested for drug trafficking) made a financial investment (life insurance) of \$250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of \$250,000 in three cash installments. The insurance broker did not report the delivery of that amount and deposited the three installments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three checks from a bank account under his name, totaling \$250,000, thus avoiding the raising suspicions with the insurance company.
- Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place

and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean check from the institution. On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

- An insurance company was established by a well-established insurance management operation. One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary. In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that the payment route out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured, the Russian insurance company.
- A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around \$400,000 deposited with a life insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account is frozen.

Reinsurance

- An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer cover of an investment firm in country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that - although drug money would be laundered by a payment received from the reinsurer - the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.
- A state insurer in country A sought reinsurance cover for its cover of an airline company. When checking publicly available information on the company it turned out that the company was linked to potential war lords and drug traffickers. A report was made to the law enforcement authorities.

Return Premiums

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

- A number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time
- Return premium being credited to an account different from the original account
- Requests for return premiums in currencies different to the original premium, and
- Regular purchase and cancellation of policies.

Overpayment of Premiums

Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by check or wire transfer to be made. A money launderer may well own legitimate assets or businesses as well as an illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

The ***overpayment of premiums***, has, been used as a method of money laundering. Insurers and agents should be especially vigilant where:

- The overpayment is over a certain size (say \$10,000 or equivalent)
- The request to refund the excess premium was to a third party
- The insured is in a jurisdiction associated with money laundering and
- Where the size or regularity of overpayments is suspicious.

High Brokerage/Third Party Payments/Strange Premium Routes

High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with example of unusual premium routes.

Claims

A claim is one of the principal methods of laundering money through insurance. Outlined below are examples of where claims have resulted in reports of suspected money laundering and terrorist financing:

- A claim was notified by the assured, a solicitor, who was being sued by one of his clients. The solicitor was being sued for breach of confidentiality, which led to the client's creditors discovering funds that had allegedly been smuggled overseas. Documents indicated that the solicitor's client might be involved in tax evasion, currency smuggling and money laundering. A claim was notified relating to the loss of high value goods whilst in transit. The assured admitted to investigators that he was fronting for individuals who wanted to invest "dirt money" for a profit. It is

believed that either the goods, which were allegedly purchased with cash, did not exist, or that the removal of the goods was organized by the purchasers to ensure a claim occurred and that they received “clean” money as a claims settlement.

- Insurers have discovered instances where premiums have been paid in one currency and requests for claims to be paid in another as a method of laundering money.
- During an on-site visit, an insurance supervisor was referred to a professional indemnity claim that the insurer did not believe was connected with money laundering. The insurer was considering whether to decline the claim on the basis that it had failed to comply with various conditions under the cover. The insurance supervisor reviewed the insurer’s papers, which identified one of the bank’s clients as being linked to a major fraud and money laundering investigation being carried out by international law enforcement agencies.
- After a successful High Court action for fraud, adjusters and lawyers working for an insurer involved in the litigation became aware that the guilty fraudster was linked to other potential crimes, including money laundering.

Assignment of Claims

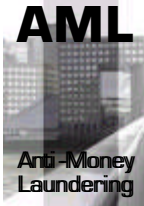
In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer. The launderer promises to pay these businesses, perhaps in cash, money orders or travellers cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payments. In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege. The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.

Non-life insurance – fraudulent claims

- Police in Country A uncovered a case of stolen car trafficking where the perpetrators provoked accidents in Country B to be able to claim the damages. The proceeds were laundered via public works companies. A network consisting of two teams operated in two different regions of Country A. Luxury vehicles were stolen and given false number plates before being taken to Country B. An insurance contract was taken out in the first country on these vehicles. In Country B, the vehicles were deliberately written off and junk vehicles with false number plates were bought using false identity documents to be able to claim the damages from the insurance firms in Country A. Around a hundred luxury stolen vehicles were used in this scheme to claim the damages resulting from the simulated or intentional accidents that were then fraudulently declared to the insurance firms. The total loss was over \$2.5 million. The country in which the accidents occurred was chosen because its national legislation provided for prompt payment of damages. On receipt of the damages, the false claimants gave 50% of the sum in cash to the leader of the gang who invested these sums in Country B. The investigations uncovered bank transfers amounting to over \$12,500 per month from the leader’s accounts to the country in question. The

money was invested in the purchase of numerous public works vehicles and in setting up companies in this sector in Country B. Investigations also revealed that the leader of the gang had a warehouse in which luxury vehicles used for his trafficking operation were stored. It was also established that there was a business relationship between the leader and a local property developer, suggesting that the network sought to place part of its gains into real estate.

- An individual purchases an expensive new car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an “accident” with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honors the claim on the policy by paying off the loan on the vehicle. Thereafter, the organization running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of \$2 million from similar fraud schemes carried out by terrorist groups.



A FINAL WORD TO AGENTS

You have just read about some fairly involved anti-money laundering rules and regulations. This is a problem agents have never had to deal with before, but, since 9/11, it is a different world requiring different action.

While it's true that the new insurance regulations do not require insurance agents and brokers to establish anti-money laundering programs or to report suspicious transactions themselves; it is also clear that life insurance agents and brokers will have an important role to play in insurance companies' anti-money laundering programs because they have direct contact with customers and are thus often in the best position to gather information and detect suspicious activity.

Insurance companies and their distribution partners must collaborate in preventing money laundering. The new rules require life insurance companies to integrate agents and brokers into their anti-money laundering programs and to monitor the agents' compliance with the programs.

The preamble to the rules states that if efforts to integrate agents into insurance company programs are ineffective, FinCEN (The U.S. Treasury) may reconsider its decision and then **require** agents and brokers to establish their own programs.

In other words, if we as agents do not cooperate now, there may a whole lot of additional reporting to do later. And, violations could be severe and costly.

INDEX

A final word to agents	45
Agents and brokers, new AML rules	14
Anti-money laundering controls	29
Anti-money laundering requirmts	22
Anti-money laundering regulations	9
Anti-money laundering training	15
Assignment of claims	43
Bank Secrecy Act 1970	9
Business relationship	31
Civil liability	28
Claims	42
Compliance	18
Compliance officer	18
Covered products	21
Customer due diligence	29
Customer due diligence measures	30
Definition, money laundering	5
Developing technologies	36
Disclosure, Suspicious Activity Rpts	28
FAQ's, anti-money laundering rules	20
Federal Crimes Enforcement Net	20
Financial institutions	10
Fraudulent claims	43
History of money laundering	4
HR 3199	10
Identification & verification	32
Identification & verification, methods	34
Indicators & examples of AML	37
Insurance companies, target for ML	6
Intermediaries	40
Internal controls	23
Legal persons and arrangements	35
Life insurance	38
Methods, identification/verification	34
Money laundering legislation	9
Money laundering legislation & ins	12
Money laundering, definition	5
Money laundering, insurance target	6
Money laundering, three stages	4
Monitoring an adequate program	24
New anti-money laundering rules	14
New rules, agents & brokers	14
New technologies, difficult identity	36
Non-life insurance	39
Obligation to identify	26
Ongoing training	23
Overpayment of premiums	42
Red flags	17
Reinsurance	41
Report of cash payments	25
Return of premiums	42

Risk profile	30
SEC exemption	19
Suspicious Activity Reports	14
Suspicious Activity Reports & agents	26
Third party payments	42
Three stages of money laundering	4
Timing of identification & verification	32
Training of agents	24
Transactions or trigger events	33
Transactions, trigger or attention	33
USA Patriot Act	10
Violations of Bank Secrecy Act	19
Vulnerabilities, insurance companies	6