Powered by ExamFX - Online Training & Assessment

Select Chapter

Study Chapter | Practice Question | Quiz

Introduction to Anti-Money Laundering

Money laundering has been around for centuries, for example, when shopkeepers attempted to hide their fortunes from their rulers to avoid taxes and seizure of property. Even in modern times, money laundering in various forms has existed and U.S. financial institutions have had obligations and responsibilities under laws designed to limit money laundering. Prior to the passage of the USA PATRIOT Act in 2001, insurance companies were not affected by these laws, but part of the USA PATRIOT Act requires that insurance agents selling "covered products" receive anti-money laundering training.

A. Definition of Money Laundering

Money laundering is defined as the process of converting funds obtained through criminal activity into what appears to be legitimately acquired money and integrating it into the national and/or international financial systems. This can be done in countless ways, and as anti-money laundering rules and procedures tighten, criminals tend to develop new and more unique ways around them.

B. Learning Objectives

The purpose of this course is to educate agents on their responsibilities as they relate to the USA PATRIOT Act. Upon completion of this course, you will be able to

- Explain the 3 phases of money laundering;
- Identify the types of insurance products most likely to be employed in a money laundering scheme;
- Explain an agent's responsibility for reporting suspicious activity; and
- Explain the red flags of money laundering as they relate to the utilization of insurance products.

Chapter Complete

Laws and Use of Life Insurance in Money Laundering

A. Bank Secrecy Act (1970)

The Bank Secrecy Act (BSA) was established in 1970, and most notably, required banks and other financial institutions to maintain records and report large cash or cash equivalent transactions of more than $10,000.

Initially, the reporting was required only for single transactions. However, as a way to circumvent filing the **Currency Transaction Report** (CTR) money launderers would structure the deposits into multiple, smaller transactions. This loophole was closed with the passing of the Money Laundering Control Act in 1986 as it mandated that multiple transactions totaling more than $10,000, by or on behalf of any person during any one business day, must be reported. These transactions are tracked as they enter, leave and circulate within the United States and provide a paper trail of the activity, sources and scope. The reports aid in the investigations of money laundering by various government agencies and law enforcement.

B. Expansion of Anti-Money Laundering Laws

The BSA is considered the foundation of the anti-money laundering laws; however, the following laws have been enacted to broaden its scope and strengthen enforcement mechanisms:

- Money Laundering Control Act (1986);
- Anti-Drug Abuse Act of 1988;
- Annunzio-Wylie Anti-Money Laundering Act (1992);
- Money Laundering Suppression Act (1994);
- Money Laundering and Financial Crimes Strategy Act (1998); and
- Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).

The body of U.S. anti-money laundering laws has expanded to establish money laundering as a federal crime, strengthen the penalties for BSA violations, and require financial institutions and other businesses to improve, review and verify compliance with the regulations. Stricter policies resulted in the requirement for **Suspicious Activity Reports** (SARs) to report suspicious activities or violations of the BSA. The term **financial institution** has grown to include other businesses over the years, and while it expanded to car dealers and real estate closing personnel in 1988 with the Anti-Drug Abuse Act of 1988, insurance companies were not part of that definition until the passing of the USA PATRIOT Act in 2001. Even then it only included insurance companies with "covered products," those that contain a **cash value**.

C. USA PATRIOT Act (2001)

In the wake of the September 11, 2001, terrorist attacks on the United States, Congress passed the **Unity and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001** (USA PATRIOT Act). The Act expanded the Bank Secrecy Act even further in several areas. However, for the purpose of this course, we will focus on the impact it has had on the insurance industry.

In addition to criminalizing the financing of terrorist activities, the Act also required insurance companies to establish anti-money laundering programs in an effort to prevent insurance products and services from being utilized in money laundering and terrorist financing schemes. (While money laundering generates funding through illicit activities, terrorist financing can also originate from legitimate income sources, such as charities.) Money laundering can be an essential element in terrorist financing by providing portable capital for ideological purposes.

D. Traditional Steps in Money Laundering

Traditionally, the goal of money laundering is to take funds derived through illicit means and integrate these funds into the U.S. financial system. Criminals have developed many creative and intricate ways to have these funds ultimately surface as “clean” money.

This process essentially involves the following three steps, which can occur independently, simultaneously, or sequentially:

1. Placement: The first step of laundering money is placement. The intent is to introduce the illegal funds (often in the form of currency) into the financial system without attracting the attention of financial institutions or law enforcement. This is the most difficult phase for the criminals since funds are most vulnerable to exposure and seizure at this point. Placement methods include converting money to other financial instruments such as money orders, cashier’s checks, or wire transfers to avoid detection. Other methods include structuring deposit amounts to dodge reporting requirements, or combining funds from legal and illegal sources in the same account or financial product. Structuring is a component of most money laundering schemes since the majority of cases begin with launderers trying to convert cash to legitimate funds. The definition of structuring, as set forth in 31 CFR 1010.100 (xx) states, “a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the [CTR filing requirements].” “In any manner” includes, but is not limited to, dividing a single currency sum exceeding $10,000 into smaller amounts of less than $10,000 to avoid triggering the reporting requirements of the law.

2. Layering: The second step of the money laundering process is layering. This step involves moving funds around throughout the financial system, often times in a complex series of transactions to conceal the source and muddle the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or transferring funds to and through numerous accounts in one or more financial institutions. Think of the sleight of hand shell game where the three cups placed upside down are shuffled around to confuse the player trying to follow which cup contains the hidden item.

3. Integration: Having gotten through the placement and layering steps successfully, money launderers move on to the integration phase. Here, the funds appear to be legitimate through additional transactions. These transactions further remove the funds from their illegal origins and the money surfaces back in the possession of the criminals involved as they make purchases, donations and investments.

1. How Life Insurance Products Can be Used by Money Launderers

One of the most notorious examples of money laundering using insurance products occurred in the state of Florida. This actual case illustrates how all 3 steps in money laundering occurred and howinsurance products were employed at the center of the scheme.

News Release U.S. Department of State:

A 2-year federal investigation dubbed Operation Capstone revealed that Colombian drug traffickers were purchasing and quickly liquidating investment-grade insurance policies to generate income that appeared to be the proceeds of legitimate insurance products. *(Source U.S. Department of State)*

Operation Capstone exposed a sophisticated criminal scheme that targeted life insurance companies in the United States, the Isle of Man, and other locations where some $80 million worth of Colombian drug proceeds have been laundered over the past few years. This two-year multinational investigation, involving the Bureau of Immigration and Customs Enforcement (ICE), the Isle of Man Customs and Excise Service, and Colombia's *Departamento Administrativo de Seguridad (DAS),* revealed that Colombian drug trafficking organizations, through a small number of insurance brokers, were purchasing investment-grade life insurance policies in the United States, the Isle of Man, and other locations, with cartel associates as the beneficiaries. These policies were funded with tens of millions of dollars' worth of drug proceeds sent (in the form of checks and wire transfers) to insurance companies by third parties around the globe. When a company receives payments for its products or services in the form of wire transfers, checks, or cash from random third parties who have no connection to the transaction, it is a clear signal that money is being laundered by drug traffickers via the insidious Black Market Peso Exchange (BMPE).

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

Operation Capstone resulted in numerous enforcement actions around the globe. ICE agents in Miami seized approximately $9.5 million, while a grand jury indicted five Colombian nationals for laundering approximately $2 million worth of drug proceeds through insurance companies. The Colombian DAS seized roughly $20 million worth of insurance policies, bonds, and cash, and arrested nine individuals. Panamanian authorities froze $1.3 million in local accounts based on evidence uncovered in Colombia.

E. Terrorist Financing vs. Traditional Money Laundering Activity

According to the Federal Financial Institutions Examination Council, “The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence.” Terrorist groups often utilize substantial sums of liquid funds to carry out their terrorist acts. Funds used by terrorist groups are often employed in various countries simultaneously and mobility of funding is a critical component to terror acts. The global financial system provides the mobility needed by terror groups, so money laundering is integral to terrorist activities.

Terrorists finance their activities through both illicit and legitimate sources. Illegal activities, such as extortion, kidnapping, and narcotics trafficking, are a major source of funding for terror groups. Other illegal activities engaged in by terrorist groups include smuggling, fraud, theft (including identity theft), robbery, use of conflict diamonds, and improper use of charitable or relief funds. (“Conflict diamonds” aka “blood diamonds” originate from areas controlled by forces or factions opposed to legitimate and internationally recognized governments, and are used to fund military action in opposition to those governments, or in contravention of the decisions of the UN Security Council.) In the case of charitable or relief contributions, donors may have no knowledge that their donations have been diverted to support terrorist causes.

Although the motivation differs between traditional money launderers and terrorist financiers, the methods used to fund terrorist operations are similar to those methods used by criminals that launder funds. For example, terrorist financiers use currency smuggling, structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers.

Chapter Complete

Insurance Company Responsibilities

A. Suspicious Activity Reports (SARs)

Since money laundering using insurance products can and does occur, it's understandable that insurance companies providing covered products would be classified as "financial institutions" and subject to anti-money laundering laws. A component of those laws is the requirement to detect and report suspicious activity by filing suspicious activity reports on Form SAR-IC (the IC refers to Insurance Company). Companies are required to file a SAR-IC if a suspicious transaction:

- Is conducted or attempted by, at or through an insurance company; or
- Involves the threshold level of $5,000 as a single transaction or an aggregate.

These SAR-ICs are submitted to FinCEN, the Financial Crime Enforcement Network. FinCEN is the designated administrator of the Bank Secrecy Act. The Director of FinCEN has the authority to administer, implement, and enforce compliance with the BSA and other related regulations. The bureau's responsibilities are to detect and deter financial crimes.

Insurance companies are required to file a SAR-IC if the company knows or suspects any of the following about a transaction:

- Involved funds are derived from illegal activity intended to violate or evade federal law or regulation or avoid any transaction reporting;
- Is designed to avoid the reporting requirements of the BSA;
- Has no business or apparent lawful purpose; or
- Involves the company to facilitate criminal activity.

The insurance company has **30 days** from the initial detection of the suspicious activity to file a SAR-IC. An additional 30 days can be granted if the suspect cannot be identified; however, all SAR-ICs must be filed within 60 days. The insurance company is required to **maintain SAR-IC reports** and supporting documents for **5 years.** Failure to comply with the rules for mandatory reporting of suspicious activity can result in substantial penalties for the insurance company.

With the volume of business processed by an insurance company on a daily basis, monitoring these transactions can be a daunting task. Most insurance companies rely on analytic software that measures transactions against a customer risk profile. When a transaction is flagged in the system, it will then undergo greater scrutiny by the AML department. The investigation can then lead to a resolution or to the filing of the SAR-IC.

1. SAR-IC Reporting and Confidentiality

It is not the agent or broker's responsibility to file suspicious activity reports; that is the responsibility of the AML Compliance Officer/Director of the insurance company.

However, the agent or broker is generally closer to the customer and may be the one to first sense possible red flags when interacting with the client. It would be the agent's responsibility at that time to report their suspicion to the AML Compliance Officer, or at a minimum, to their manager.

The insurer may request additional information from the agent or broker relative to the suspicious activity; however, the insurer and the agent are prohibited by law from disclosing to anyone the information filed, or even the fact that a SAR-IC report has been filed. As the subject of the SAR-IC, this would most definitely include the customer. An exception to this would be sharing information with the appropriate law enforcement and regulatory agencies.

B. Red Flags - Activity That May Indicate Money Laundering or Terrorist Financing

Some examples of suspicious activities are what FinCEN calls red flags. The following are examples of potentially suspicious activities, or "red flags" for both money laundering and terrorist financing. These activities may warrant a more critical examination by the insurance company's AML department or officer to determine whether the activity is suspicious or for which there does not appear to be a reasonable or legal purpose. If an agent is unsure if a customer's actions constitute suspicious activity they should consult with the insurance company AML compliance officer.

1. Point of Service Red Flags

The following are considered point-of-service red flags:

- A customer uses unusual or suspicious identification documents that cannot be readily verified.
- A customer provides an individual taxpayer identification number after having previously used a Social Security number.
- A customer uses different taxpayer identification numbers with variations of his or her name.
- A business owner is reluctant, when establishing a new account, to provide complete information about the nature and purpose of their business or the names of its officers and directors, or information on its business location.
- The customer's background differs from that which would be expected on the basis of his or her business activities.
- The policy applicant seems concerned with potential transaction reporting requirements
- A customer provides answers to questions that are inconsistent or provides answers that are misleading.
- A customer is more concerned about the withdrawal charges that might apply to a policy than they are with the investment performance, indicating they may be planning to surrender or borrow against the policy soon after issued.
- A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents. Note: Most insurance companies, as a matter of policy, will not accept cash for premium payments.
- A customer purchases a product that appears outside the customer's normal range of financial wealth or estate planning needs.
- Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include secondhand endowment and bearer insurance policies.

- A customer uses multiple currency equivalents (e.g., cashier's checks, money orders, and traveler's checks) from different banks and money services businesses to make insurance policy or annuity payments.
- A customer is unusually curious about insurance company compliance procedures
- A customer purchases multiple policies where insured differs on each policy
- A customer appears to be acting as an agent for an undisclosed principal, but is reluctant or declines to provide information about the undisclosed principal with a legitimate commercial reason to do so.
- The customer is representing a business, but has difficulty describing the nature of their business or lacks basic knowledge of the industry that they purport to be engaged in.
- The customer wants to purchase multiple policies under a single name or multiple names without a plausible reason for doing so.
- The customer is only willing to meet at a location that is unusual.
- The customer insists on paying only in cash or cash equivalents, or asks for exemptions from the insurer's cash or cash equivalent policies.
- The address on the check tendered is different from the insured's address.
- The customer attempts to pay with a third party check.
- A policyowner provides false or inaccurate information about the source of funds used for policy payments.

2. Policy Service Red Flags

While there are many legitimate reasons for policyowners to request policy service in the areas of loans, surrender, and ownership changes, the agent should be on alert for the following red flags. This is not an all-inclusive list of potential suspicious activity.

- The customer exercises the right to refund during the free look period, particularly if the premium was paid with cash or cash equivalents.
- A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.
- A customer borrows against or surrenders a recently issued permanent life insurance policy; particularly when loan or surrender proceeds are made payable to apparently unrelated third parties.
- A customer borrows against or surrenders a recently issued permanent life insurance policy, particularly when the purchase was a single premium tendered in the form of cash or cash equivalent.
- Lack of concern over surrender charges or fees when requesting a policy surrender.
- A request to transfer ownership of a policy to an unrelated individual.
- A pattern of large premium payments (particularly cash or cash equivalents) follow by loan requests of similar amounts.
- A business customer engages in transactions that lack business sense or are inconsistent with their investment strategy as stated at policy inception.

C. Bank Secrecy Act Suspicious Activity Report

Now that we have an understanding of the identification and reporting requirements for suspicious activities, let's take a look at the recent volume of SAR-ICs as reported to FinCEN by the insurance companies.

Filings by Year & Month by an Insurance Company *
March 1, 2012, through December 31, 2016

Month	2012	2013	2014	2015	2016
January	0	219	211	159	176
February	0	211	265	174	204
March	0	189	273	180	231
April	11	320	290	183	213

May	13	262	277	192	205
June	17	318	232	177	181
July	89	280	231	209	180
August	60	307	223	207	171
September	41	196	206	184	197
October	155	236	172	196	194
November	158	261	155	209	218
December	182	267	200	235	219
Subtotal	**726**	**3,066**	**2,735**	**2,305**	**2,389**
Total Filings	**11, 221**				

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

Number of Filings by Type of Suspicious Activity by an Insurance Company * March 1, 2012, through December 31, 2016

1	Multiple transactions below BSA recordkeeping threshold	2,799	**11.81%**
2	ACH	2,782	**11.74%**
3	Suspicion concerning the source of funds	2,221	**9.37%**
4	Suspicious use of noncash monetary instruments	997	**4.21%**
5	Alters transaction to avoid BSA recordkeeping requirement	994	**4.19%**
6	Transaction with no apparent economic, business, or lawful purpose	991	**4.18%**
7	Insurance-Other	817	**3.45%**
8	Two or more individuals working together	712	**3.00%**
9	Elder financial exploitation	682	**2.88%**
10	Other suspicious activities - Other	658	**2.78%**
11	Identity theft	647	**2.73%**
12	Provided questionable or false documentation	644	**2.72%**
13	Little or no concern for product performance penalties, fees, or tax consequences	539	**2.27%**
14	Money laundering - Other	524	**2.21%**

15	Embezzlement/theft/disappearance of funds	490	2.07%
16	Forgeries	489	2.06%
17	Suspicious use of multiple locations	440	1.86%
18	Check	429	1.81%
19	Structuring - Other	411	1.73%
20	Proceeds sent to unrelated third party	401	1.69%
21	Account takeover	387	1.63%
22	Excessive or unusal cash borrowing against policy/annuity	376	1.59%
23	Wire	358	1.51%
24	Suspicious EFT/wire transfers	313	1.32%
25	Multiple transactions below CTR threshold	310	1.31%
26	Fraud - Other	304	1.28%
27	Suspicious use of multiple accounts	303	1.28%
28	Suspicious termination of policy or contract	247	1.04%
29	Suspicious use of third-party transactors (straw-man)	237	1.00%
30	Transaction out of pattern for customer(s)	234	Less than 1%
31	Unauthorized electronic intrusion	222	Less than 1%
32	Mail	202	Less than 1%
33	Misuse of position or self-dealing	193	Less than 1%
34	Suspicious life settlement sales insurance (e.g., STOLI's, Viaticals)	144	Less than 1%

35	Suspicious designation of beneficiaries, assignees or joint owners	129	Less than 1%
36	Excessive insurance	122	Less than 1%
37	Unclear or no insurable interest	106	Less than 1%
38	Identification documentation - Other	96	Less than 1%
39	Mortgage fraud - Other	90	Less than 1%
40	Counterfeit Instrument (other)	85	Less than 1%
41	Appraisal fraud	84	Less than 1%
42	Refused or avoided request for documentation	61	Less than 1%
43	Changes spelling or arrangement of name	45	Less than 1%
44	Healthcare	42	Less than 1%
45	Single individual with multiple identities	35	Less than 1%
46	Alters transactions to avoid CTR requirement	34	Less than 1%
47	Multiple individuals with same or similar identities	33	Less than

			1%
48	Credit/Debit Card	32	Less than 1%
49	Misuse of "free look"/cooling-off/right of rescission	30	Less than 1%
50	Suspected public/private corruption (domestic)	22	Less than 1%
51	Pyramid scheme	20	Less than 1%
52	Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements	18	Less than 1%
53	Consumer Loan	17	Less than 1%
54	Suspected public/private corruption (foreign)	12	Less than 1%
55	Terrorist financing - Other	11	Less than 1%
56	Bribery or gratuity	10	Less than 1%
56	Suspicious exchange of currencies	10	Less than 1%
57	Customer cancels transaction to avoid BSA reporting and recordkeeping requirements	8	Less than 1%
57	Securities/Futures/Options - Other	8	Less than 1%
		7	

58	Suspicious receipt of government payments/benefits		Less than 1%
59	Suspicion concerning the physical condition of funds	6	Less than 1%
60	Casinos - Other	5	Less than 1%
60	Mass-marketing	5	Less than 1%
61	Business loan	4	Less than 1%
61	Insider trading	4	Less than 1%
61	Suspicious use of informal value transfer system	4	Less than 1%
61	Trade Based Money Laundering/Black Market Peso Exchange	4	Less than 1%
62	Known or suspected terrorist/terrorist organization	3	Less than 1%
63	Foreclosure fraud	2	Less than 1%
63	Market manipulation/wash trading	2	Less than 1%
64	Misappropriation	1	Less than 1%
64	Reverse mortgage fraud	1	Less than 1%
64	Unlicensed or unregistered MSB	1	Less than 1%

* Some SAR-IC filings may list multiple suspicious activities.

Number of Filings by Product Type(s) involved in the suspicious activity by an Insurance Company *
March 1, 2012, through December 31, 2016

Product Type	2012	2013	2014	2015	2016
Bonds/Notes	0	1	0	0	0
Commercial mortgage	0	1	2	1	0
Commercial paper	0	2	0	0	0
Credit card	4	10	13	5	7
Debit card	1	2	5	3	1
Forex transactions	11	0	0	0	0
Futures/Options on futures	0	0	0	0	0
Hedge fund	0	1	0	0	0
Home equity loan	0	0	0	0	0
Home equity line of credit	0	1	0	0	0
Insurance/Annuity products	294	1,082	1,118	1,389	1,935
Mutual fund	1	1	4	8	14
Options on securities	0	0	0	0	0
Penny stocks/Microcap securities	0	0	3	1	1
Prepaid access	0	0	2	1	1
Residential mortgage	0	2	1	1	2
Security futures products	1	1	0	1	0
Stocks	0	2	1	2	4
Swap, hybrid, or other derivative	0	0	0	0	0
Other	77	89	143	66	69

* Some SAR-IC filings may list multiple suspicious activities.

Number of Filings by instrument type(s)/payment mechanisms involved in the suspicious activity by an Insurance Company *
March 1, 2012, through December 31, 2016

Type of Instrument Type(s)/Payment Mechanism(s)	2012	2013	2014	2015	2016
Bank/Cashier's check	33	130	118	140	144
Foreign currency	1	29	7	13	17
Funds transfer	44	156	107	233	441
Gaming instruments	0	0	0	1	0
Government payment	3	1	0	1	0
Money orders	144	628	873	998	890
Personal/Business check	149	455	580	766	723
Travelers checks	0	2	3	1	1
U.S. Currency	29	91	158	226	113
Other	10	47	39	46	45

* Some SAR-IC filings may list multiple instrument type(s)/payment mechanism(s).

D. Cash Payments Over $10,000 – Report Form 8300

In addition to the Suspicious Activity Report, insurance companies must also file **Form 8300,** Report of Cash Payments Over $10,000 Received in a Business or Trade. Similar to the banks' Currency Transaction Report (CTR), insurance companies are required to file Form 8300 to report the receipt of cash or cash equivalents (money orders, cashier's checks) more than $10,000. The transaction can be a single transaction or multiple, associated transactions. These transactions must be reported within **15 days** of receipt of the cash. Filing of form 8300 does not satisfy the insurance company's duty to file a SAR-IC; therefore, there are situations where both reports would need to be filed. The substantial penalties when an insurance company fails to report the cash transaction(s) are **equal to the greater of $25,000 or an amount equal to the cash received, not to exceed $100,000**.

IRS Form **8300** (Rev. August 2014)
Department of the Treasury Internal Revenue Service

Report of Cash Payments Over $10,000 Received in a Trade or Business

▶ See instructions for definition of cash.
▶ Use this form for transactions occurring after August 29, 2014. Do not use prior versions after this date.
For Privacy Act and Paperwork Reduction Act Notice, see the last page.

FinCEN Form **8300** (Rev. August 2014)
OMB No. 1506-0018
Department of the Treasury Financial Crimes Enforcement Network

1 Check appropriate box(es) if: a ☐ Amends prior report; b ☐ Suspicious transaction.

Part I Identity of Individual From Whom the Cash Was Received

2 If more than one individual is involved, check here and see instructions . . . . . ▶ ☐

3 Last name	4 First name	5 M.I.	6 Taxpayer identification number

7 Address (number, street, and apt. or suite no.)	8 Date of birth (see instructions) ▶ M M D D Y Y Y Y

9 City	10 State	11 ZIP code	12 Country (if not U.S.)	13 Occupation, profession, or business

14 Identifying document (ID)	a Describe ID ▶ c Number ▶	b Issued by ▶

Part II Person on Whose Behalf This Transaction Was Conducted

15 If this transaction was conducted on behalf of more than one person, check here and see instructions . . . . . ▶ ☐

16 Individual's last name or organization's name	17 First name	18 M.I.	19 Taxpayer identification number

20 Doing business as (DBA) name (see instructions)	Employer identification number

21 Address (number, street, and apt. or suite no.)	22 Occupation, profession, or business

23 City	24 State	25 ZIP code	26 Country (if not U.S.)

27 Alien identification (ID)	a Describe ID ▶ c Number ▶	b Issued by ▶

Part III Description of Transaction and Method of Payment

28 Date cash received M M D D Y Y Y Y	29 Total cash received $ .00	30 If cash was received in more than one payment, check here . . . ▶ ☐	31 Total price if different from item 29 $ .00

32 Amount of cash received (in U.S. dollar equivalent) (must equal item 29) (see instructions):

a	U.S. currency	$ .00	(Amount in $100 bills or higher $ .00)
b	Foreign currency	$ .00	(Country ▶)
c	Cashier's check(s)	$ .00	Issuer's name(s) and serial number(s) of the monetary instrument(s) ▶
d	Money order(s)	$ .00	
e	Bank draft(s)	$ .00	
f	Traveler's check(s)	$ .00	

33 Type of transaction

a	☐ Personal property purchased	f	☐ Debt obligations paid
b	☐ Real property purchased	g	☐ Exchange of cash
c	☐ Personal services provided	h	☐ Escrow or trust funds
d	☐ Business services provided	i	☐ Bail received by court clerks
e	☐ Intangible property purchased	j	☐ Other (specify in item 34) ▶

34 Specific description of property or service shown in 33. Give serial or registration number, address, docket number, etc. ▶

Part IV Business That Received Cash

35 Name of business that received cash	36 Employer identification number

37 Address (number, street, and apt. or suite no.)	Social security number

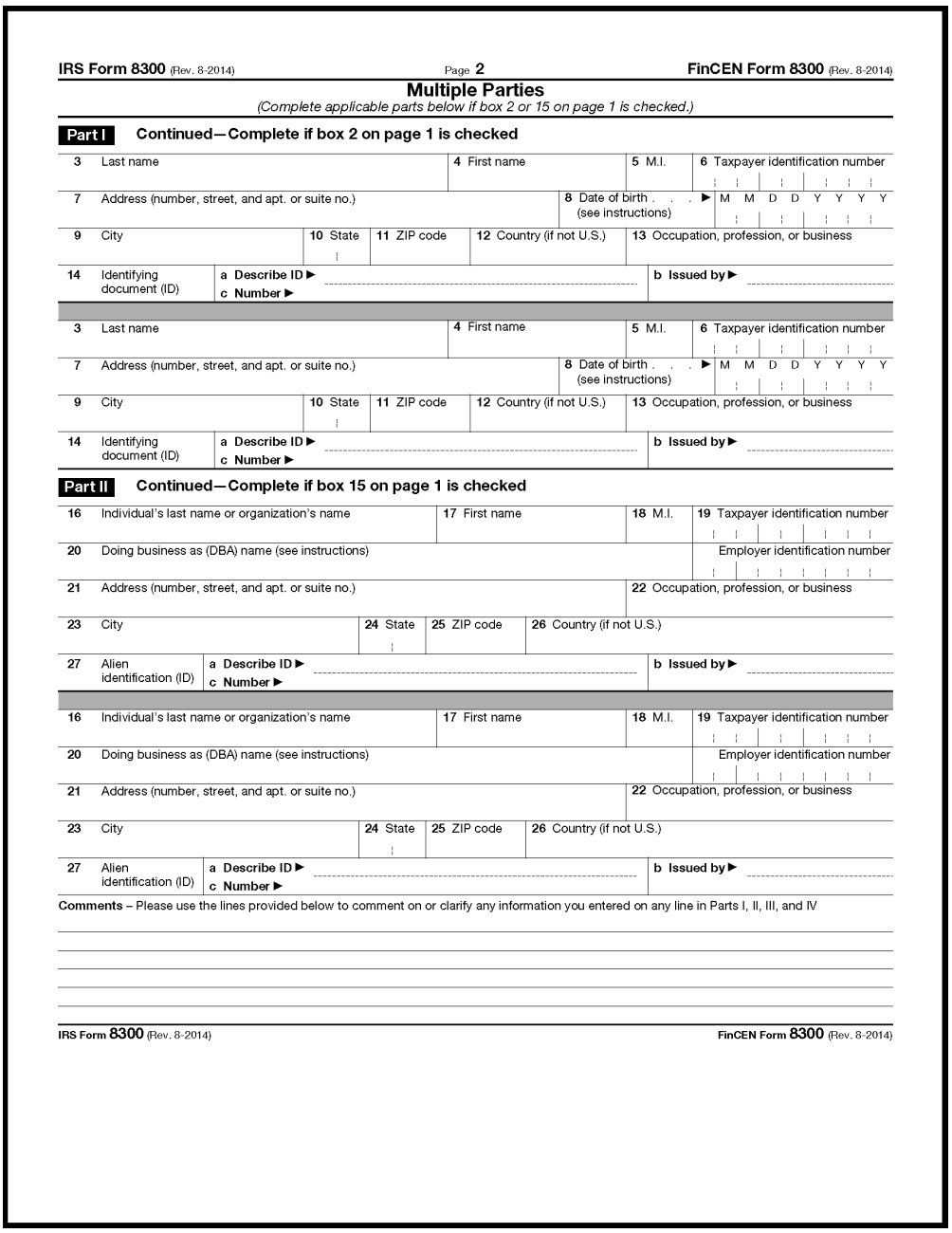
38 City	39 State	40 ZIP code	41 Nature of your business

42 Under penalties of perjury, I declare that to the best of my knowledge the information I have furnished above is true, correct, and complete.

Signature ▶ _____ Authorized official Title ▶ _____

43 Date of signature M M D D Y Y Y Y	44 Type or print name of contact person	45 Contact telephone number

IRS Form **8300** (Rev. 8-2014) Cat. No. 62133S FinCEN Form **8300** (Rev. 8-2014)



IRS Form 8300 (Rev. 8-2014) Page **2** **FinCEN Form 8300** (Rev. 8-2014)

Multiple Parties

(Complete applicable parts below if box 2 or 15 on page 1 is checked.)

Part I **Continued—Complete if box 2 on page 1 is checked**

3 Last name		4 First name		5 M.I.	6 Taxpayer identification number
7 Address (number, street, and apt. or suite no.)			8 Date of birth . . . ► (see instructions)		M M D D Y Y Y Y
9 City	10 State	11 ZIP code	12 Country (if not U.S.)	13 Occupation, profession, or business	
14 Identifying document (ID)	a Describe ID ► c Number ►			b Issued by ►	

3 Last name		4 First name		5 M.I.	6 Taxpayer identification number
7 Address (number, street, and apt. or suite no.)			8 Date of birth . . . ► (see instructions)		M M D D Y Y Y Y
9 City	10 State	11 ZIP code	12 Country (if not U.S.)	13 Occupation, profession, or business	
14 Identifying document (ID)	a Describe ID ► c Number ►			b Issued by ►	

Part II **Continued—Complete if box 15 on page 1 is checked**

16 Individual's last name or organization's name		17 First name		18 M.I.	19 Taxpayer identification number
20 Doing business as (DBA) name (see instructions)					Employer identification number
21 Address (number, street, and apt. or suite no.)				22 Occupation, profession, or business	
23 City	24 State	25 ZIP code	26 Country (if not U.S.)		
27 Alien identification (ID)	a Describe ID ► c Number ►			b Issued by ►	

16 Individual's last name or organization's name		17 First name		18 M.I.	19 Taxpayer identification number
20 Doing business as (DBA) name (see instructions)					Employer identification number
21 Address (number, street, and apt. or suite no.)				22 Occupation, profession, or business	
23 City	24 State	25 ZIP code	26 Country (if not U.S.)		
27 Alien identification (ID)	a Describe ID ► c Number ►			b Issued by ►	

Comments – Please use the lines provided below to comment on or clarify any information you entered on any line in Parts I, II, III, and IV

IRS Form 8300 (Rev. 8-2014) **FinCEN Form 8300** (Rev. 8-2014)

E. OFAC – Office of Foreign Assets Control

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFAC maintains several different lists of blocked or sanctioned individuals, businesses, or countries that are important to U.S. insurance companies. Not all of these lists denote suspected money launders or terrorist financiers and organizations. Some of the lists relate to foreign policy sanctions that impose various limitations on

services and transactions that can occur with residents or businesses within a particular country.

1. OFAC List of Specially Designated Nationals (SDN)

The list that we will focus on for the purposes of this course is the list of Specially Designated Nationals (commonly referred to as the SDN list). According to OFAC, The SDN list is comprised of “individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them.” It should be noted, that as used in OFAC’s description of the SDN List, “U.S. persons” encompasses not only individuals within the U.S., but also any U.S. business.

The most common insurance company violation of anti-money laundering laws is processing a transaction with an individual, institution or country on the OFAC SDN list.

OFAC updates all of their lists (sanctions and the SDN list) as they receive new information from various branches of the government such as Treasury or Intelligence, or additional orders in the form of legislation from Congress, or emergency orders from the President. According to OFAC, these lists are updated “as frequently as a few times a week or as rarely as once in a month.” The law states that an insurance company must block transactions within 10 days of an SDN being added to the SDN list. The reason for the 10-day requirement is to freeze the account before it can escape U.S. Jurisdiction. OFAC does not stipulate how often an insurer scrubs their customer list against the SDN list, but they do offer guidance and the penalties for a violation are steep.

Once an SDN is added to the SDN list the insurer is prohibited for “providing any service” to the SDN. Following is an excerpt from guidance provided by OFAC as part of their outreach program to U.S. insurers: "If you receive an application from an SDN for a policy, you are under an obligation not to issue the policy. Remember that when you are insuring someone, you are providing a service to that person. You are not allowed to provide any services to an SDN. If the SDN sends a deposit along with the application, you must block the payment. If you receive an application from a party on one of OFAC's other sanctions lists, please review the specific treatment prohibitions associated with that list carefully before taking any action."

2. Countries Subject to OFAC Sanctions

In addition to the list of individuals on the SDN maintained by OFAC, there are a number of countries that are subject to sanctions. Below is a list of countries subject to various levels of sanctions by OFAC. This list is current as of April 2018 and is subject to change. OFAC provides several methods for financial institutions to link to the current SDN and other sanctions lists in order to avoid violations by doing business with a blocked individual, group, or country. The various methods available for an insurer to use the resources provided by OFAC to scrub their lists of customers (both existing and new customers) against the OFAC lists are collectively termed software interdiction.

Countries subject to various levels of sanctions by OFAC are as follows:

- Balkans

- Belarus
- Burundi
- Burma (Myanmar)
- Central African Republic
- Cuba
- Darfur
- Democratic Republic of the Congo
- Iran
- Iraq
- Lebanon
- Libya
- Somalia
- South Sudan
- Syria
- Ukraine / Russia
- Venezuela
- Yemen
- Zimbabwe

3. Insurer Responsibilities to Block Transactions with SDNs

As was discussed earlier, when an agent or insurer encounters a red flag and generates a SAR-IC they are prohibited from communicating to the customer that they have filed a SAR-IC. However, if an insurer blocks a transaction with a customer because they are on the SDN list, that can be communicated to the customer. Since it will most often be the insurer that discovers the link between the customer and SDN list, this communication will usually originate from the insurer and not the agent.

4. When OFAC Compliance Contravenes State Insurance Law

State insurance laws address issues such as an insurer's ability to decline to enter into contracts, ability to withhold claims payments, or timeliness in responding to policyholder requests for access to nonforfeiture values, or ability to cancel policies. Complying with OFAC blocking requirements will sometimes cause an insurer to violate state insurance laws. OFAC blocking and sanctions are enforced as a result of federal laws, which always preempt state laws. Since the passage of the USA PATRIOT Act, many states have amended their insurance codes to include exceptions for insurers when acting to comply with federal laws related to money laundering or OFAC sanctions.

5. Insurer Responsibility at Policy Issue

At time of policy issue the insurer must check the policyowner and beneficiary against the SDN list and if the customer is on the SDN list, the insurer is obligated to block policy and to file a SAR-IC.

If at application the customer is not on the SDN list, but lists a beneficiary who is on the list, the policy cannot be issued with that particular beneficiary, and the insurer must file a SAR-IC report.

6. Insurer Responsibility while Policy Is in Force

If the customer or beneficiary is not on the SDN list at the time of policy issue, but is added to the SDN list while the policy is in force, the policy must be **immediately frozen and reported to OFAC**. The insurer can then send a letter to the policyholder informing them that the policy has been frozen and directing them to OFAC for answers to any questions they may have. Following is guidance from OFAC in the form of the text that could be used for that letter, *"If you send any more premiums, we are required under applicable U.S. laws and regulations to place such funds in a blocked account. If you*

have any questions, please contact the U.S. Department of Treasury's Office of Foreign Assets Control."

7. Loan or Distribution Request with SDN Designated as Payee

If the policyowner requests a loan or distribution (depending on policy type) and requests that the check be made payable to a SDN, the transaction must be blocked and a SAR-IC filed. In this example it is likely that OFAC will also require the insurer to freeze the account because it is also possible that, upon investigation, the customer may also be added to the SDN list.

8. Change of Beneficiary to SDN

If, while the policy is in force, the policyowner requests to change ownership of the policy, or to change the beneficiary, or to assign the policy as collateral to a SDN, the transaction should be blocked and a SAR-IC filed.

9. Insurer Responsibility when Paying Claims

When an insurer pays a claim on a policy they should check the payee against the SDN to make sure the payee is not on the SDN list.

F. FATF – Financial Action Task Force

While the U.S. regulators have adopted many FATF policies, FATF is not an enforcement or regulatory body, and therefore, does not investigate any money laundering activities. The Financial Action Task Force is an international body that was established in 1989. Their role is to combat money laundering and terrorist financing by setting global standards through the promotion of policies and procedures that safeguard the stability of the international financial system.

Chapter Complete

Establishment of Anti-Money Laundering Programs

A. Section 352 of USA PATRIOT Act

Section 352 of the USA PATRIOT Act requires all insurance companies issuing or underwriting covered products to establish an anti-money laundering (AML) program applicable to its covered products. The AML program should be structured so that it is reasonably expected to prevent the insurance company from being utilized to launder money.

1. Covered Products

The USA PATRIOT Act defines covered products as

- 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 of covered products within the law uses a functional approach. It includes insurance products that have the same types of features and characteristics that make permanent life insurance and annuity products more at risk of being used for money laundering, such as, having a cash value or investment feature. Insurance products that do not build cash values such as term life insurance, property and casualty insurance and health insurance are not considered covered products.

Exceptions

There are some insurance products that build cash values that are not considered covered products under the USA PATRIOT Act because of a combination of products structure and circumstances surrounding their sale and funding. The following insurance products are specifically **excluded** from the definition of covered products by the USA PATRIOT Act:

- Group insurance products (group life or annuities);
- Products offered by charitable organizations, such as charitable annuities;
- Contracts of indemnity and structured settlements (including workers compensation payments).

2. Requirements of the Producer

Insurance agents are not required to have their own anti-money laundering programs, but the insurers for whom they sell covered products will require them to participate in anti-money laundering training as part of the insurer's AML program. Insurance agents are in a unique position to make observations due to their contact with the customer and, as such, will often be exposed to information about the source of investment assets, the nature of the clients, and the objectives for which the insurance products

are being purchased. Insurance agents have an important role to play in assisting the insurance company to prevent money laundering which include the following:

- Be familiar with the insurance company's AML program;
- Know the red flags and report suspicious activity to the AML officer of the insurance company;
- Provide additional client information upon request by the AML officer
- Know the acceptable forms of payment;
- Be prepared to refuse the business or suspend the transaction if criminal activity is suspected;
- Maintain complete and accurate records in client file; and
- Do not disclose suspicious activity or the filing of a SAR-IC to anyone, including the customer, outside of AML department, law enforcement or government agencies.

Confidentiality is of the utmost importance as alerting a customer that their actions constitute suspicious activity is a direct violation of AML laws and may result in civil and criminal penalties as well as potentially put the agent in danger.

3. Requirement of Insurance Company AML Program

The AML Program must be in writing, approved by senior management, and available to the Treasury Department for inspection if requested. In addition to the establishment of AML programs, Section 352 of the USA PATRIOT Act requires that as part of the AML program insurance companies:

- Designate an AML Compliance Officer;
- Develop risk-based policies, procedures and controls to identify money laundering;
- Integrate insurance agents into their AML programs;
- Establish an AML training program and provide ongoing training; and
- Undergo periodic independent testing and verification of the effectiveness of the AML program.

The AML compliance officer does not have to be a full-time position unless the transaction volume or level of risk dictates. The AML compliance office should have the necessary authority to oversee the day-to-day activities of the AML program.

Independent testing and review must be accomplished by either an independent third party or insurance company personnel who do not work specifically for the AML compliance officer. The testing and review process should include a review of the risk-based decisions made in system design as well as testing of the day-to-day functions of the AML program. A written report of the findings, including any recommendations, should be sent to senior management.

While all insurance companies selling covered products are required to establish an anti-money laundering program, it is possible for the programs to vary widely from one company to another. The AML program should take into account the covered products sold, types of customers, distribution channels and geographic area served. Agents are not required to establish their own AML programs, but they must be familiar with the AML program of each insurer whose covered products they sell.

4. Risk-Based Approach to AML Program

While section 352 of the USA PATRIOT Act requires that the AML program be developed using a risk-based approach, money launderers and terrorist organizations often have considerable knowledge of life insurance companies and products, and take extreme measures to hide their financial activities that make them difficult to

distinguish from legitimate insurance transactions. A risk-based approach is designed to make it more difficult for these criminals to make use of life insurance companies due to the increased focus on the identified higher risk activities.

5. Factors Influencing Risk-Based Approach

A risk-based approach will allocate resources to areas where money laundering or terrorist financing is most likely to occur. The risk-based approach to establishing an anti-money laundering program can vary greatly depending on the products sold, types of customers serviced, and many other factors. Some of the items that are considered by the insurer when developing a risk-based approach include

- Distribution channel where transaction originates;
- Customer characteristics;
- Method of payment;
- Size and frequency of transaction;
- Type of insurance product involved; and
- Existence of a beneficial owner other than the customer.

6. Forms of Payment Accepted

One of the first decisions many insurers made in order to comply with AML regulation was to revise and formalize their policies and procedures related to the acceptance of payments. Since the first step in money laundering is placement, many insurers feel that one critical way to limit risk is to identify the types of payments that are most likely to represent an attempt to inject illicit funds into an insurance product. Once these forms of payment are identified, the insurer can decide to either not accept these forms of payment or subject them to additional scrutiny. While the forms of payment vary by insurance company, the following chart outlines the predominant methods of acceptable and unacceptable payments. To identify acceptable payment types by company, an agent must consult their company's individual AML policy. Cash and cash equivalents are the most common forms of payments used in the placement stage of money laundering and are subject to the highest level of scrutiny by financial institutions.

Acceptable Payment Methods	Unacceptable Payment Methods
Personal Checks drawn on a domestic bank	Cash
Company Checks drawn on a domestic bank on behalf of company employees	Third party checks
Checks from other financial institutions made payable to the insurance company on behalf of the insured (common in Section 1035 exchanges and custodian-to-custodian transfers)	Checks or cash equivalents drawn on foreign banks
Check from a close relative for the benefit of the insured or a minor in the case of a custodial account	Starter checks when the customer information is not imprinted on the check
Bank checks (Cashier checks)	Travelers checks

Money Orders	Checks drawn on a foreign bank
Wire transfers from acceptable financial institutions	Endorsed money orders, cashier checks or other cash equivalents
Foreign checks only if paid through a domestic bank in US currency	Frequent payments outside of the normal premium policy or payment schedule

A sophisticated criminal may understand the additional focus placed on new accounts by a risk-based anti-money laundering program and their true intentions may only become evident once they begin processing unusual transactions. This makes continual monitoring of account activity an important part of the overall anti-money laundering program. Some of the triggers used by insurance companies to identify transactions requiring a closer look include the following:

- Policies surrendered during the free look period. Premium size can be used as a parameter to trigger a closer look.
- Policy assignment or use as collateral. Policy size and age of contract can be used as parameters.
- Policy surrender during surrender charge period. Policy size and timing of surrender are parameters that can be used to trigger a closer look.
- Change of policy ownership. Contract value, relationship (or lack thereof) of new owner to original owner, and size and age of contract can serve as triggers for additional review.
- Request for payments of living benefits where the payment is to be sent to an unrelated third party, a foreign financial institution, or to an entity in a high-risk country.
- A pattern of policy loans or living benefit distributions that are immediately repaid in cash or cash equivalents.

7. Customer Profiles

Another part of a risk-based anti-money laundering program is identifying customer profiles (individual or business) that are considered higher risk. The U.S. Treasury Department has provided some guidance by identifying certain types of individuals and businesses that should be considered higher risks for money laundering.

Examples of higher-risk individual customers include

- A senior official in the executive, legislative, administrative, or judicial branch of a foreign government;
- A senior official of a major foreign political party;
- A senior executive of a foreign-owned corporation; and
- Any resident, business, or official of a country that is listed on the "Non Cooperative Jurisdictions" list maintained by the Financial Actions Task Force (FATF).

Examples of higher-risk business customers include

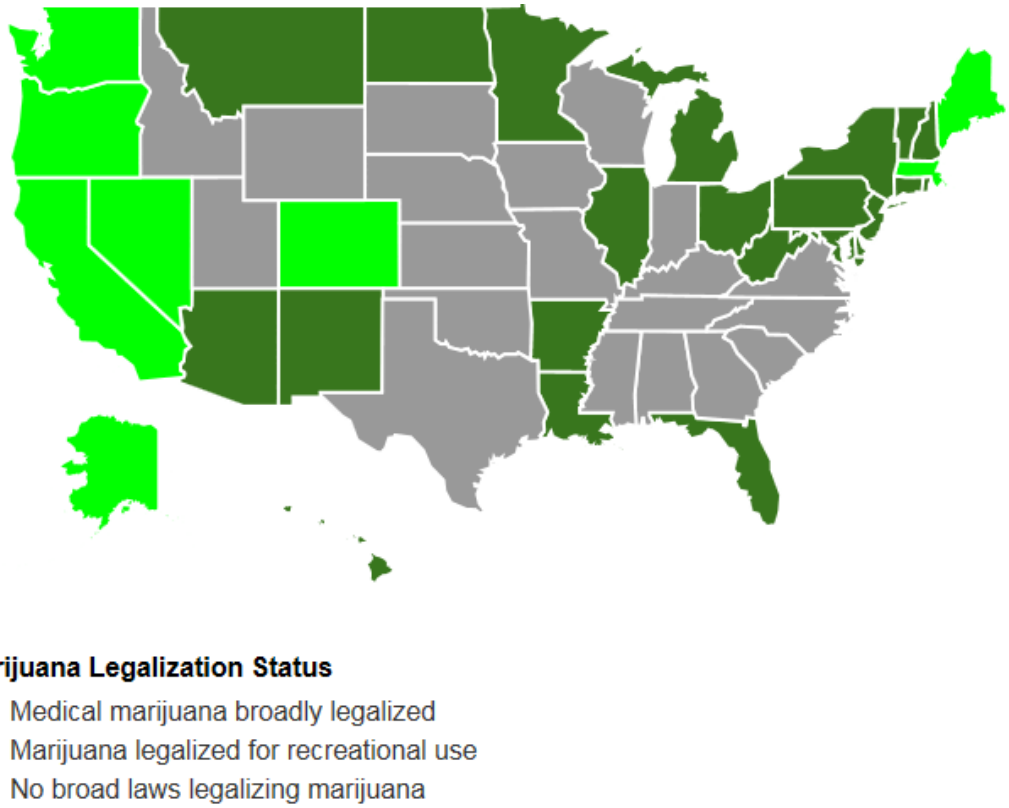
- Import/export companies;
- Pawn brokers and deposit brokers;
- A jeweler or precious metals dealer;
- Professional service providers such as lawyers and accountants, particularly when acting on behalf of a client.;

- Any cash intensive business, such as restaurants, bars, retail stores, convenience stores, strip clubs, and parking garages;
- Check cashing facilities (money service businesses);
- Currency exchange houses; and
- Offshore corporations and banks or businesses located in high-risk foreign countries (Non Cooperative Jurisdictions as identified by the Financial Actions Task Force).

Insurance companies are not prohibited from doing business with high-risk individuals or businesses, but when transacting business there should be enhanced scrutiny and due diligence.

8. Insurance Companies are Weeding Out Marijuana-Related Risks

Many insurance companies with covered products are currently on the sidelines when it comes to doing business with marijuana-related businesses. Currently, 30 states and the District of Columbia have legalized marijuana-related activity, whether it be for medicinal use only or (as in 8 states) for recreational purposes as well.



SOURCE: Governing.com

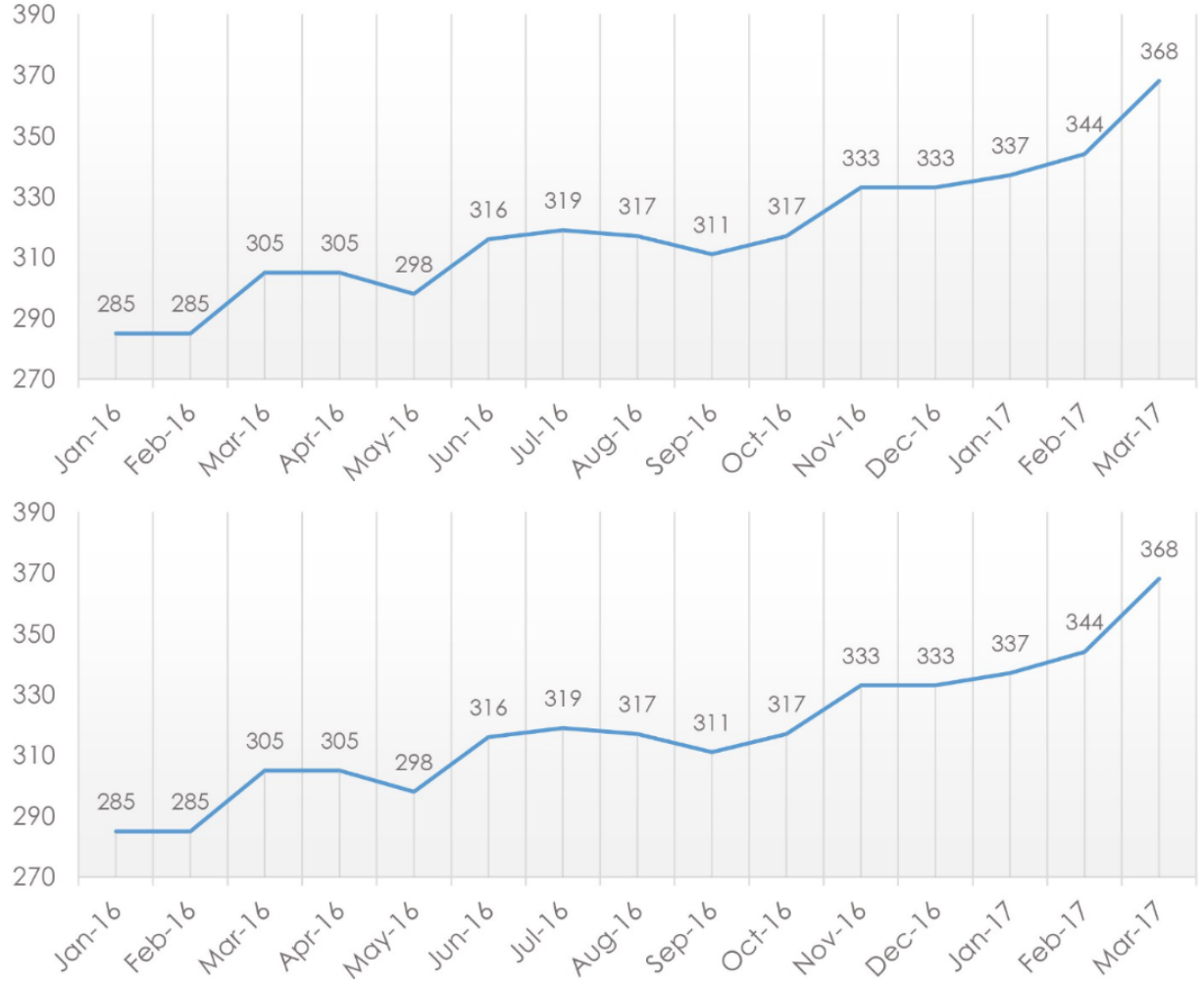
The problem is, regardless of the state laws, federal laws still make it illegal to manufacture, distribute or dispense marijuana under the Controlled Substances Act.. In January 2018, Attorney General Jeff Sessions rescinded a prior memo issued by the Obama Administration which discouraged federal prosecutors from enforcing federal marijuana laws in states where it was legal.Sessions directed all U.S. Attorneys to use “previously established prosecutorial principles that provide them all the necessary tools to disrupt criminal organizations, tackle the growing drug crisis, and thwart violent crime across our country” and reiterated that marijuana is a dangerous drug and that the illegal distribution and sale of marijuana is a serious crime that provides a significant source of revenue to large-scale criminal enterprises, gangs and cartels.

On February 14, 2014, FinCEN issued guidance, “BSA Expectations Regarding Marijuana-Related Businesses,” to financial institutions, including life insurance and

annuity companies, requiring those companies doing business with persons or companies involved in the manufacturing, selling or distribution of marijuana to file a special SAR. The "marijuana limited" SAR indicates that the customer is engaged in a marijuana-related business but no other suspicious activity has been identified. While the individuals or companies may be licensed and properly operating their business according to state laws, many insurance companies have instructed their agents to not accept applications from anyone known to be in a marijuana-related business.

However, as the medical and recreational use of marijuana becomes more widespread, more and more financial institutions are expected to find ways to service the financial needs of that industry. In 2017, FINCEN reported the number of depository institutions actively banking marijuana businesses in the United States (measured by the number of SARs filed).

Number of Depository Institutions Actively Banking Marijuana Businesses in the United States (Reported in SARs)



390
370
350
330
310
290
270
285
285
305
305
298
316
319
317
311
317
333
333
337
344
368
Jan-16
Feb-16
Mar-16
Apr-16
May-16
Jun-16
Jul-16
Aug-16
Sep-16
Oct-16
Nov-16
Dec-16
Jan-17
Feb-17
Mar-17

B. Customer Identification Program

Section 326 of the USA PATRIOT Act requires covered insurance companies to establish and maintain a Customer Identification Program (CIP). Section 326 does not apply to insurers selling only covered products that are not also FINRA supervised products. *For example*, an insurer selling covered products in the form of fixed annuities or traditional cash value life insurance products that do not require selling

agents to also be securities-licensed, are not specifically required under Section 326 to establish a customer identity program.

However, there are parts of the Bank Secrecy Act that require insurance companies to obtain and retain identifying information from customers in certain situations. The bottom line is insurance companies must obtain and retain relevant and appropriate customer information necessary to administer an effective anti-money laundering program.

1. CIP Program Requirements

The CIP must include elements covering customer identity, customer identity verification, customer screening and records retention. These requirements of the CIP are often referenced using the term "**Know Your Customer**" (KYC).

The first step in a CIP is to determine and verify the identity of the customer. Since the customer can be an individual or a business, there are separate sets of procedures and processes for each of these types of customers.

The process of identity verification (IDV) requires the following:

When the **customer is an individual**:

- Customer full legal name;
- Date of birth;
- Customer's physical address. This should be the personal residence of the customer not a P.O. Box, commercial mailbox, or company address.
- Social Security Number or Tax ID #. Most insurance companies require customers to complete and sign the IRS form W9: Request for Taxpayer Identification and certification.

When the **customer is a business**, many of the same documents are required as when the customer is an individual. The insurance company must verify the identity of the individual purporting to represent the business entity, and the existence of the business entity. There are 2 steps to the business identification process. The first step is to verify that the business does exist and the second step is to verify that the customer is legally empowered to represent the business. The following documents are used in this process:

- If the business is a Corporation, present Certified Articles of Incorporation;
- If the business is a Limited Liability Company or Limited Liability Partnership, present an Operating Agreement;
- If the business is a General Partnership, present a Partnership Agreement;
- If the customer is a trust, present a Trust Document;

In addition to these general business documents, some insurance companies will also require documentation of organizational meeting, certified financial statements, or a business license.

Identity Verification and Record Retention

Verification of this information should include a photo ID, such as a state issued driver's license, state issued photo ID, U.S. Passport, U.S. Military ID, Resident Alien ID (green card), or some foreign government ID cards.

The agent is not specifically required under the various AML laws to retain a copy of the photo ID, but some insurance companies do require the agent to retain a copy. Therefore, the agent should become familiar with all requirements of their insurers' anti-money laundering programs, including any recordkeeping requirements.

When the agent is doing business with a customer via phone, mail, or Internet, the agent will likely not meet with the customer face to face. It is also possible that the agent will meet with a customer, but the customer is purchasing an insurance product for an individual that the agent does not meet. In these cases the customer's identity can be verified by the insurance company using other methods.

An insurance company can use several methods to verify customer identity other than the agent actually seeing a photo ID. These methods are called non-documentary identity verification. Usually non-documentary identity verification includes one or more of the following methods:

- Insurance company personnel contact the customer after the account is opened and verify that address, phone number and social security number or taxpayer identification number are correct.
- Insurance company personnel compares the information provided by the customer with data available from a third party such as a credit bureau, or government entity.
- Checking references provided by customer with other financial institutions
- Physical verification of the customer's address (for an individual or a business).
- Using various other online identity verification procedures.

The insurance company is not required to determine the veracity of the customer identity information or documents provided. Specifically the insurance company may rely on government issued (U.S. or state government) ID's to establish identity.

It should be noted that from a reputational risk perspective some insurers will require additional identity documentation or verification. Using a risk-based approach, some insurance companies will use both non documentary methods of identity verification and verification of identity through a photo ID for certain customers and/or transaction types.

Special Designated Nationals

An office of the U.S. Treasury, The Office of Foreign Asset Control (OFAC), maintains and publishes a list of Special Designated Nationals (SDN). This list represents individuals and companies owned or controlled by, or acting for or on behalf of, countries targeted by the U.S. Treasury Department. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers that are considered threats to national security. Their assets of SDNs are blocked and U.S. persons and businesses are generally prohibited from dealing with them. Financial entities (including insurance companies) must check this SDN list against all existing and new customers.

C. Bank Sales of Insurance

Insurance products are typically sold to bank customers through networking arrangements with an affiliate, an operating subsidiary, or other third-party insurance providers. Banks are also interested in providing cross-selling opportunities for customers by expanding the insurance products they offer. Typically, banks take a role as a third-party agent selling covered insurance products. The types of insurance products sold may include life, health, property and casualty, and fixed or variable annuities.

When an insurance agent or broker already is required to establish a BSA/AML compliance program under a separate requirement under BSA regulations (e.g. bank or securities broker requirements), the insurance company may rely on that compliance program to address issues at the time of sale of the covered product. However, the bank may need to establish specific policies, procedures, and processes

for its insurance sales in order to submit information to the insurance company for the insurance company's AML compliance.

Likewise, if a bank, as an agent of the insurance company, detects unusual or suspicious activity relating to insurance sales, it can file a joint SAR-IC on the common activity with the insurance company.

Chapter Complete

Penalties for Violations

A. Willful Blindness

As we begin our discussion on penalties for violations of the Bank Secrecy Act, USA PATRIOT Act, or SDN lists, it is important for agents to understand the concept of ***willful blindness***. Willful blindness in the context of a discussion of money laundering and the dealings of an insurance agent could be described by the idiom: "Turning a blind eye."

It is easy to see how an agent could be penalized for a violation of one of the various money laundering laws where it is proven that the agent "knew" that money laundering was occurring. However, the terms "deliberate indifference" and "willful blindness" have been employed in criminal and civil courts to establish that an individual did, in fact, "have knowledge" of a crime.

If we consult Black's Law Dictionary (8th edition), we see that "deliberate indifference" is defined as "*the careful preservation of one's ignorance despite awareness of circumstances that would put a reasonable person on notice of a fact essential to a crime",* and "willful blindness" is defined as *"the deliberate* avoidance *of knowledge of a crime, especially by failing to make a reasonable inquiry about suspected wrongdoing despite being aware that it is highly probable".*

B. Red Flags and Willful Blindness

As an agent, you should not look the other way and ignore red flags that might indicate money laundering is occurring, because ignorance will be a weak excuse if it turns out that money laundering was indeed being carried out. If a prosecutor is attempting to employ the concept of willful blindness in a criminal trial, the judge will, when giving the jurors their final instructions before deliberations begin, often charge the jury with a standard of "conscious avoidance" (nicknamed the ostrich instruction).

Below is the actual text of the pattern instructions published as a guide for federal judges to use when instructing the jurors relative to determining if a defendant possessed knowledge of a fact.

In deciding whether [defendant] acted knowingly, you may infer that [defendant] had knowledge of a fact if you find that he/she deliberately closed his/her eyes to a fact that otherwise would have been obvious to him/her. In order to infer knowledge, you must find that two things have been established. First, that [defendant] was aware of a high probability of [the fact in question]. Second, that [defendant] consciously and deliberately avoided learning of that fact. That is to say, [defendant] willfully made himself/herself blind to that fact. It is entirely up to you to determine whether he/she

deliberately closed his/her eyes to the fact and, if so, what inference, if any, should be drawn. However, it is important to bear in mind that mere negligence or mistake in failing to learn the fact is not sufficient. There must be a deliberate effort to remain ignorant of the fact.

The criminal actors that launder illicit funds and/or finance terrorism are often well trained in tactics designed to manipulate unknowledgeable agents, and spot those individuals who will easily compromise their standards for financial gain.

C. Penalties for Violations of BSA or USA PATRIOT Act

1. Damage to Reputation

An agent or insurance company's reputation and/or license to transact business within the financial services industry are often the first casualties when a violation of the anti-money laundering laws is discovered. Both insurers and agents can face substantial civil and criminal penalties for violations of anti-money laundering laws.

2. Penalties

Criminal penalties may include fines of up to $500,000 or twice the value of the property involved in the act, whichever is greater, and incarceration in a federal penal institution for up to **20 years**.

Civil penalties can be as high as $10,000 or the value of the property involved in the act, whichever is greater. In addition, asset forfeitures of any ill-gotten gains can be imposed. These penalties are for each violation. If a continuing pattern of conduct is considered to be a deliberate and ongoing criminal enterprise the consequences can be much more severe.

Under the Bank Secrecy Act, additional civil and criminal penalties can be imposed, including

- Up to 5 years imprisonment;
- Civil fines of up to $250,000; or
- Both: fines and imprisonment.

The USA PATRIOT Act has increased the civil and criminal penalties that can be imposed for some sections of the Bank Secrecy Act up to twice the amount of the property involved or $1,000,000. The Department of the Treasury website shows that for calendar year 2017, OFAC imposed fines of $119,517,845 for 16 separate enforcement actions.

3. Penalty Determination

When deciding how to proceed with criminal prosecution or civil penalties after a violation has been discovered, OFAC uses a measured approach and takes the following into account:

- Was the violation self-reported by the individual or financial institution;
- The degree of willfulness or recklessness exhibited by the agent or institution;
- Whether the agent or institution had knowledge;
- Whether the agent or institution had intent;
- If reckless disregard or failure to exercise minimal caution existed;
- If there was concealment or collusion on the part of multiple parties within the financial institution;
- If there can be established a deliberate pattern of misconduct; or
- If upper management was involved.

4. Penalty Mitigation

Items that are considered and can serve to mitigate penalties during an OFAC investigation of a violation include the following:

- If the violation was self-reported;
- The scope and level of sophistication of the violation;
- The effectiveness and quality of OFAC compliance program at time of violation;
- The degree to which the insurer practiced software interdiction;
- The timing of the violation with respect to when the prohibited individual, institution or country was added to the OFAC lists;
- Corrective remedial action taken by financial institution after discovery of the violation;
- Conduct of thorough review/investigation to detect and identify other possible violations; or
- Degree of cooperation with OFAC investigators.

D. In the News

FinCEN Penalizes U.S. Bank National Association for Violations of Anti-Money Laundering Laws

Feb. 15, 2018

The Financial Crimes Enforcement Network (FinCEN), in coordination with the Office of the Comptroller of the Currency, and the U.S. Department of Justice, announced the assessment of a $185 million civil money penalty against U.S. Bank for willful violations of several provisions of the Bank Secrecy Act (BSA). U.S. Bank's obligation will be satisfied by payment of $70 million to the U.S. Department of the Treasury with the remaining amount satisfied by payments in accordance with the DOJ's actions. Since 2011, U.S. Bank willfully violated the BSA's program and reporting requirements by failing to establish and implement an adequate anti-money laundering program, failing to report suspicious activity, and failing to adequately report currency transactions.

Banks are required to conduct risk-based monitoring to sift through transactions and to alert staff to potentially suspicious activity. Instead of addressing apparent risks, U.S. Bank capped the number of alerts its automated transaction monitoring system would generate to identify only a predetermined number of transactions for further investigation, without regard for the legitimate alerts that would be lost due to the cap.

"U.S. Bank is being penalized for willfully violating the Bank Secrecy Act, and failing to address and report suspicious activity. U.S. Bank chose to manipulate their software to cap the number of suspicious activity alerts rather than to increase capacity to comply with anti-money laundering laws," said FinCEN Director Kenneth A. Blanco. "U.S. Bank's own anti-money laundering staff warned against the risk of this alerts-capping strategy, but these warnings were ignored by management. U.S. Bank failed in its duty to protect our financial system against money laundering and provide law enforcement with valuable information."

U.S. Bank systemically and continually devoted an inadequate amount of resources to its AML program. Internal testing by U.S. Bank showed that alert capping caused it to fail to investigate and report thousands of suspicious transactions. Instead of removing the alert caps, the bank terminated the testing. U.S. Bank also allowed, and failed to monitor, non-customers conducting millions of dollars of risky currency transfers at its branches through a large money transmitter. In addition, U.S. Bank

filed over 5,000 Currency Transaction Reports (CTRs) with incomplete or inaccurate information, impeding law enforcement's ability to identify and track potentially unlawful behavior.

U.S. Bank also had an inadequate process to handle high-risk customers. As a result, customers whom the bank identified or should have identified as high-risk were free to conduct transactions through the bank, with little or no bank oversight. By not having an adequate process in place to address high-risk customers, U.S. Bank failed to appropriately analyze or report the illicit financial risks of its customer base. These failures precluded the bank from adequately addressing the risks that such customers posed, including filing timely suspicious activity reports that law enforcement investigators rely upon to recognize and to pursue financial criminals.

Chapter Complete

Powered by ExamFX - Online Training & Assessment

Select Chapter

Study Chapter | Practice Question | Quiz

Case Studies

A. Case Study #1

Sally Johnson contacted insurance agent, John Gilford, to purchase an annuity. When John met with Sally she presented him with a check from her personal checking account in the amount of $15,000 to purchase the annuity. Over the 2-week period immediately after the annuity was issued, Sally sent John additional premium deposits in the form of four money orders, three for $2,000 each and one for $1,000, totaling $7,000. This behavior indicated a red flag to John, so he contacted his company's AML department with this information. It is later determined that Sally had been selling bootlegged merchandise at a local flea market on a cash basis. John was correct to notify his AML Officer.

Here, the examples are Placement, Structuring, Layering and Integration:

- **Placement:** When Sally introduced the cash into the financial system by purchasing money orders.
- **Structuring:** When Sally purchased the money orders for an amount less than $3,000 to avoid a CTR transaction when purchasing money orders or traveler's checks, and when she submitted money orders totaling less than $10,000 to circumvent the filing of Form 8300 by the insurance company.
- **Layering:** By purchasing the money orders then purchasing the annuity, Sally attempted to conceal the origin of the funds by using different transaction vehicles within the financial system.
- **Integration:** Once Sally requests money from her annuity and receives a check written by a U.S. financial institution (insurance company), the funds appear legitimate.

B. Case Study #2

Insurance agent Marty Jones recently sold a single premium whole life insurance policy to a client, Mr. James Singleton. Two months after the policy was issued, Mr. Singleton requested that the ownership be changed to another person. When Marty inquired about the relationship between Mr. Singleton and the new owner, Mr. Singleton suggested the relationship was his private information. The response raised a red flag for Marty, so he notified his AML department. The AML department then filed a SAR-IC, and an investigation ensued. It was discovered that the new policyowner was listed on the SDN list.

C. Case Study #3

Janice Lofton sold a $75,000 annuity to a customer, only for the customer to request 1 month later to liquidate the annuity. Janice reminded the customer that there would be a 12% surrender charge, or $9,000 of the proceeds, if the policy was cancelled at this

time. The customer had little concern for the loss of funds due to the surrender charge, but was extremely curious if the company would be required to file the transaction with the government. The client's anxiety about the compliance procedures, coupled with the lack of concern for the $9,000 surrender charge, prompted Janice to report the cancellation request to her AML department.

D. Case Study #4

Robert, an insurance agent, sold a fixed annuity, a variable annuity and a whole life insurance policy to Kathy, a new customer. Kathy made an initial deposit of $9,000 into the fixed annuity, $8,000 into the variable annuity and $5,000 into the life insurance policy. About a month later, during the 45-day free-look period, Kathy surrendered both annuities and requested refund checks payable to an unrelated third party off shore. Three weeks later, she cashed in the life insurance policy and once again requested a check payable to an unrelated third party off shore.

These transactions raised a red flag for Robert for several reasons: all three products were terminated early; the refund checks were issued to an unrelated third party, and the transactions appeared to serve no business or personal purpose. Robert suspects that Kathy is using insurance products to launder money, and reports the transactions to the insurance company's AML Compliance Department that will file a Suspicious Activity Report (SAR-IC) within 30 calendar days.

E. Case Study #5

Jane, the general manager of a small insurance agency, employs another agent, Tim, as an administrative assistant and to process walk-in business. Tim manages the office when Jane is out calling on prospects, which is most of the time. One day, Tim was alone in the office and Dave, a 20-year-old man with no dependents, stopped in and purchased a $1,000,000 whole life policy with $30,000 in cash. After the completion of the application, Tim deposited the cash in the agency's checking account, wrote a check to the insurance carrier, sent off the application, and went about his business. He never mentioned to Jane, or the AML Department of the insurance carrier, that the life insurance policy was purchased with cash.

The purchase of such a large policy appears to be inconsistent with the insurance needs of a young man with no dependents. That, coupled with the cash payment, should have caused enough suspicion for Tim to contact the insurance carrier's AML Department to file a SAR-IC. Further, Tim was unaware that a Form 8300 must be filed within 15 days for cash transactions of $10,000 or more, so a report was never filed. To prevent future violations, the insurance carrier should review its Anti-Money Laundering Program, written policies and procedures, and provide appropriate training for its agents and brokers.

F. Case Study #6

Gaylord contacted Matt, an insurance agent in Pennsylvania, to purchase a variable annuity. When they met, Matt was surprised to learn that Gaylord was from California. During the meeting Gaylord was vague about his investment objectives and showed little concern for the types of investments in the separate account. Even his social security number (121-12-1212) seemed suspect. In addition, the initial deposit of $80,000 was made with a wire transmitted from a foreign bank. Matt wondered why Gaylord, a California resident, purchased an annuity in Pennsylvania, a place so far from his home. It also concerned him that Gaylord showed almost no interest in the investment characteristics of the annuity. When he saw that Gaylord's wire came from

a foreign bank, Matt decided it was time to contact annuity issuer's AML Department. The Department filed a SAR-IC.

G. Bibliography

Bank Secrecy Act/Anti-Money Laundering Examination Manual, Federal Financial Institutions Examination Council, (Board of Governors of the Federal Reserve System) 2014

Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies Frequently Asked Questions (FIN-2008-G004) plus current updates from Department of Treasury Website, Department of the Treasury: Financial Crimes Enforcement Network. https://www.fincen.gov/resources/statutes-regulations/guidance/frequently-asked-questions-anti-money-laundering-program

Pattern Criminal Jury Instructions for the District Courts of the First Circuit, Portland, ME 1997. *Jury Charging Instructions for Willful Blindness*

Guidance on Obtaining and Retaining Beneficial Ownership Information FIN-2010-G001, 2010, Department of the Treasury, Financial Crimes Enforcement Network

OFAC Regulations for the Financial Community, 2012 Department of the Treasury, Office of Foreign Asset Control

Customer Identification Programs and Banks Serving as Insurance Agents, 2006, Department of the Treasury, Financial Crimes Enforcement Network

Department of the Treasury Office of Foreign Asset Control website: used for information on currently sanctioned countries. http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

BSA Expectations Regarding Marijuana-Related Businesses FIN-2014-G001, 2014 U.S. Department of the Treasury, Financial Crimes Enforcement Network,

Blacks Law Dictionary 8th Edition, 2004 Thomson West Publishing, Rochester, New York, Bryan A Garner.

IRS/FINCEN Form 8300 and instructions (rev 8/2014) Receipt of Cash Payments Over $10,000 Received in a Trade or Business. 2014, Department of the Treasury, Internal Revenue Service.

Recommended Core Elements of an AML Training Program for Life Insurance Agents and Brokers, 2006, American Council of Life Insurers. Washington DC

Chapter Complete