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

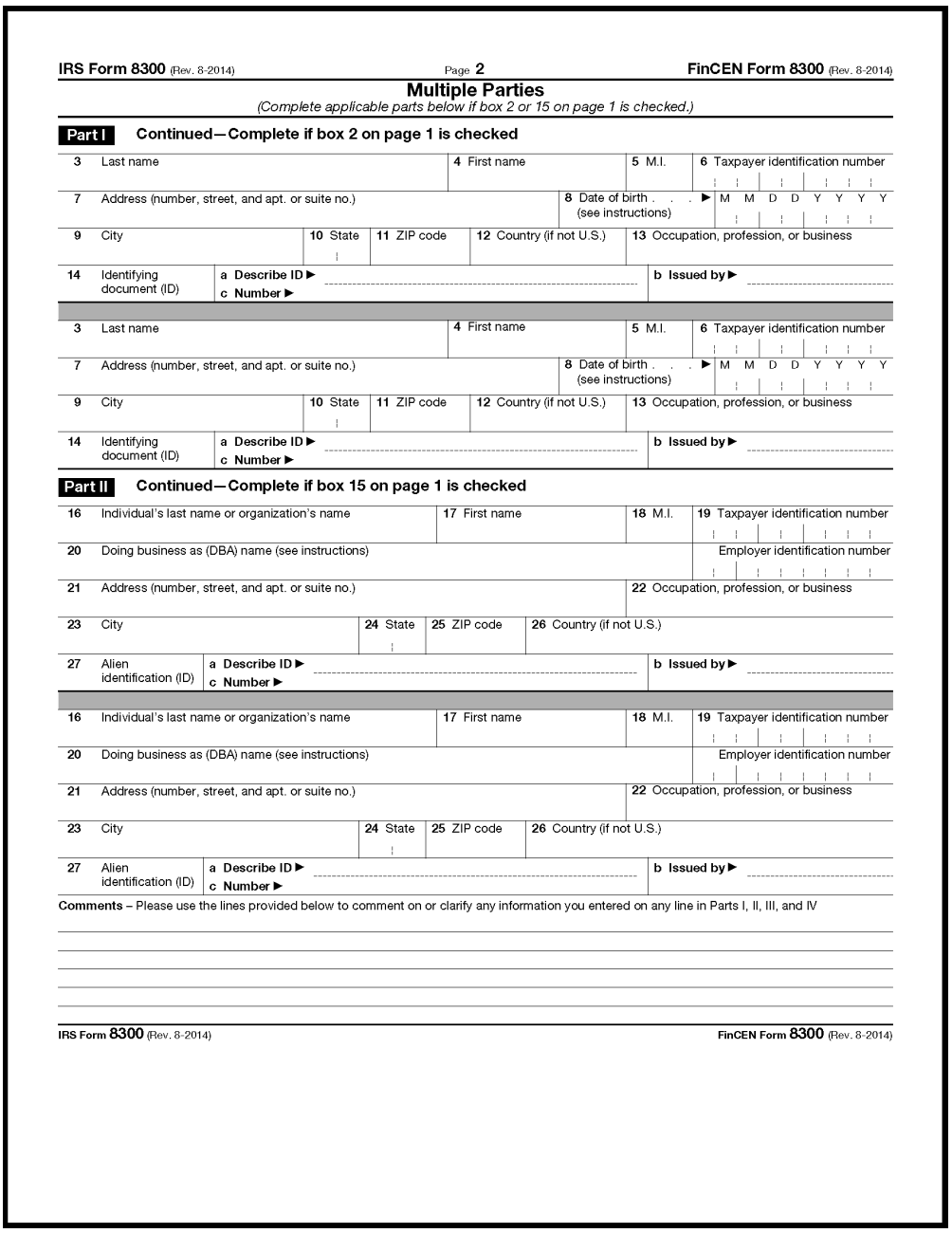
38 City	39 State	40 ZIP code	41 Nature of your business

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