

Locke Lord QuickStudy: Navigating AML and Sanctions Compliance in the Insurance Industry

Locke Lord LLP

WRITTEN BY

Ryan Last

Money laundering generally refers to financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources, or nature of their illicit activities. Money laundering facilitates a broad range of serious underlying criminal offenses and ultimately threatens the integrity of the U.S. financial system.

The Bank Secrecy Act (“BSA”), among other things, requires financial institutions to develop and implement anti-money laundering (“AML”) compliance programs. Insurance companies are deemed “financial institutions” under the BSA. The USA PATRIOT Act of 2001 (Pub. L. No. 107-56 (2001)) further directs the Secretary of the U.S. Department of the Treasury to prescribe through regulation minimum standards for such AML compliance programs and suspicious activity reporting (“AML Rules”). Issuing or underwriting “covered products” requires higher AML due diligence standards than other insurance products such as property & casualty, workers’ compensation or health insurance. “Covered Products” specifically include (i) permanent life insurance policies, other than a group life insurance policy; (ii) annuity contracts, other than a group annuity contract; and (iii) any other insurance product with cash value or investment features. To the extent that an insurance policy does not include a cash value component or investment features (“Exempt Insurance Products”), they are not Covered Products. Only insurance companies dealing in Covered Products are subject to AML Rules. FinCEN’s AML Rules regarding Covered Products are set forth at [Title 31 Subtitle B, Chapter X, Part 1025](#).

Compliance for Exempt Insurance Products

Insurance companies, whether they issue or underwrite Covered Products, continue to have AML obligations for cash and cash equivalent transactions. All U.S. persons are required to file a Form 8300 (“Report of Cash Payments Over \$10,000 in a Trade or Business”) upon receipt of more than \$10,000 in cash in a single transaction or in related transactions. Form 8300 must be filed with the U.S. Department of the Treasury’s Internal Revenue Service (“IRS”) and the Financial Crimes Enforcement Network (“FinCEN”) within 15 days of the date the cash was received. Cash includes the coins and currency of the United States and a foreign country. Cash may also include cashier’s checks, bank drafts, traveler’s checks, and money orders with a face value of \$10,000 or less, if the business receives the instrument in: (i) a “designated reporting transaction” (as defined below), or (ii) any transaction in which the business knows the customer is trying to avoid reporting of the transaction on Form 8300.

A “designated reporting transaction” is the retail sale of any of the following: (i) a consumer durable such as an

automobile, boat, or property other than land or buildings (a) suitable for personal use, (b) can reasonably be expected to last at least one year under ordinary use, (c) has sales price of more than \$10,000, and (d) can be seen or touched (tangible property); (ii) a collectible such as a work of art, rug, antique, metal, gems, stamps, or coins, or (iii) travel or entertainment, if the total sales price of all items sold for the same trip or entertainment event in one transaction or related transactions is more than \$10,000. The total sales price of all items sold for a trip or entertainment event includes the sales price of items such as airfare, hotel rooms and admission tickets.

AML compliance programs are usually coupled with sanction compliance programs because the tools used to search required lists have similar attributes.

Sanctions

All insurers, irrespective of whether they underwrite Covered Products or Exempt Insurance Products, are required to comply with U.S. sanctions laws. The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") administers and enforces U.S. economic and trade sanctions programs against targeted foreign governments, individuals, groups, and entities enacted to protect U.S. national security and promote foreign policy goals and objectives; these sanctioned parties are generally referred to as "specially designated nationals," or "SDNs." Organizations subject to U.S. jurisdiction, foreign entities that conduct business in or with the United States, U.S. persons, or persons using U.S.-origin goods or services, should develop and implement a sanctions compliance program to protect against transacting with SDNs to avoid violating U.S. sanctions laws. While each compliance program will vary depending on the company's products, customers and geographic locations, each program should incorporate the five essential components: (1) management commitment; (2) risk assessments; (3) internal controls; (4) testing and auditing; and (5) training.

In recent press, the U.S. has been expanding its use of sanctions to set and enforce foreign policy. New sanctions against Russia, China and other U.S. trading partners have been rolling out of Washington D.C. faster than automobiles off an assembly line. With these new sanctions come daily updates to the SDN lists. Many of the newly minted SDNs have significant U.S. insurable interests – U.S. branches, employees, assets and inventory.

Insurers should periodically, when writing, renewing, accepting payment or paying claims, check the names of the counterparties against the SDN lists. If there is a "match" then OFAC must be involved. Violators of U.S. sanctions can face monetary fines ranging from a few thousand dollars to several million, and/or prison of up to 30 years. One of the "red flags" that our clients have noted as a sign that a non-U.S. insured or its beneficial owner may have been added to the SDN list is a change in payor. Banks have advanced sanctions screening tools that automatically close accounts held by SDNs. Without a bank account, the SDN then generally relies on its affiliates not designated on the SDN list, such as an employee, to pay its premium.

As noted in OFAC's [FAQ 63](#), "What should an insurer do if it discovers that a policyholder is or becomes a Specially Designated National (SDN)—cancel the policy, void the policy ab initio, non-renew the policy, refuse to pay claims under the policy? Should the claim be paid under a policy issued to an SDN if the payment is to an innocent third-party (for example, the injured party in an automobile accident)? A: The first thing an insurance company should do upon discovery of such a policy is to contact OFAC Compliance. OFAC will work with you on the specifics of the case. It is possible a license could be issued to allow the receipt of premium payments to keep the policy in force. Although it is unlikely that a payment would be licensed to an SDN, it is possible that a payment

would be allowed to an innocent third party. The important thing to remember is that the policy itself is a blocked contract and all dealings with it must involve OFAC.

In the insurer's letter to the SDN policyholder, OFAC [recommends](#) the insurer instruct the policyholder as follows: "If you send any more premium, 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."

In [FAQ 64](#) OFAC advised "A workers' compensation policy is with the employer, not the employee. Is it permissible for an insurer to maintain a workers compensation policy that would cover a person on the Specially Designated Nationals (SDN) List, since the insurer is not transacting business with the SDN, but only with his/her employer?"

If an insurer knows that a person covered under the group policy is an SDN, that person's coverage is blocked, and if he or she makes a claim under the policy, the claim cannot be paid. If an insurer does not know the names of those covered under a group policy, it would have no reason to know it needed to block anything unless and until an SDN files a claim under that policy. At that point, its blocking requirement would kick in.

If an insurer knows that a person covered under a group policy is on one of OFAC's other sanctions lists, a different set of restrictions may apply. The insurer should contact OFAC if a claim is filed by an individual on one of the other sanctions lists."

Key Elements of an Effective Risk-Based Compliance Program

- 1. Risk Assessment:** A thorough risk assessment is fundamental to an effective AML and sanctions compliance program. It evaluates factors such as organizational size, jurisdictional scope, operational complexity, product offerings, and regulatory environment, defining the company's risk appetite and guiding compliance measures.
- 2. Internal Compliance Measures:** Compliance measures such as "Know Your Customer" due diligence, transaction monitoring, and employee training should be implemented to identify and address potential money laundering, sanctions violations, or other illicit activities. This includes screening mechanisms to check customers and other counterparties against U.S. sanctions lists, as well as implementing enhanced due diligence measures for high-risk customers, such as those operating in high-risk jurisdictions or politically exposed persons.
- 3. Testing of Compliance Measures:** Regular reviews of AML and sanctions compliance programs are essential components of ongoing compliance efforts. Insurance companies should stay abreast of changes in AML and sanctions related laws and regulations to ensure that their screening processes remain effective and compliant with applicable requirements.
- 4. Beneficial Ownership:** While insurance companies not dealing in Covered Products are not required to identify or verify beneficial owners, such insurance companies should adopt a risk-based approach to identifying beneficial owners of customers, considering recent enforcement actions where inadequate due diligence on beneficial owners of policyholders led to severe penalties.

Conclusion

Effective AML and Sanctions Compliance Programs are essential for all insurance companies, whether subject to BSA Rules or exempt. Regular risk assessments, responsive screening, and adaptability to changes in the business and regulatory environment are critical to mitigate risks associated with money laundering and sanctions evasion effectively.?

RELATED INDUSTRIES + PRACTICES

- [Corporate](#)
- [Insurance + Reinsurance](#)
- [International](#)
- [Sanctions + Trade Controls](#)