Anti-Money Laundering Course for the Insurance Industry

Table of Contents

Introduction

This course will familiarize producers in your organization with the anti-money laundering (AML) compliance requirements of the US Department of the Treasury. After a producer completes this course, he or she will be more equipped with recognizing and preventing money laundering - the

illegal activity used to hide the true origin and ownership of illegal cash.

This course will assist you in recognizing money laundering and terrorist financial risks. This course requires about 30 minutes to complete, and after passing the test, you'll get a certificate of completion.

This course will help producers and agencies to understand the AML rules and regulations that insurance carriers have to follow. This course provides the explanations of the methods and consequences money laundering and it consists of three parts:

- AML Basics
- Responsibilities of producer and agencies
- Suspicious activity reporting

At the end of each part, you'll be offered review questions that will test your understanding of the covered materials. Upon completion of the course, participants should be able to understand and identify money laundering processes. They will understand the personal responsibilities of a producer and will know how to report suspicious activity.

Part 1 AML Basics

In this part, you'll become familiar with some terms used in the AML rules and regulations as well as some AML-related acronyms. You'll also learn about the stages of money laundering.

The US Department of the Treasury (see https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/money-laundering) offers the following definition: *"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 financial system."*

Dirty money can take many routes - some complex, some simple, but all increasingly inventive - the ultimate goal being to disguise its source. The money can move through banks, check cashing services, money transmitters, businesses, casinos, and even be sent overseas to become clean, laundered money. The tools of the money launderer can range from complicated financial transactions, carried out through webs of wire transfers and networks of shell companies, to old-fashioned currency smuggling.

The life insurance industry creates massive flows of funds, and a portion of it may serve the criminals in their money-laundering schemes. In particular, life insurance policies offer flexible investments that can be used by some clients for disposing of large sums of cash with further recovery through legitimate channels.

The Basel Anti-Money Laundering Index is an independent annual ranking that assesses the risk of money laundering and terrorist financing around the world. According to Basel AML Index 2018 (see https://www.baselgovernance.org/sites/default/files/2019-02/basel_aml_index_10_09_2018.pdf), 64% of countries (including the USA) have a significant risk of money laundering and terrorist financing.

The Money Laundering Control Act of 1986 (Public Law 99-570) is a United States Act of Congress that made money laundering a federal crime. But even before this act, Congress has enacted multiple measures to prevent criminal money laundering.

The Bank Secrecy Act (BSA) of 1970 requires traditional banks and other financial institutions (including insurance companies) to perform anti-money laundering checks and to collaborate with the U.S. government in cases of suspected money laundering and fraud. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. BSA requires that financial institutions have a written program, perform ongoing training for personnel, and conduct monitoring for the BSA compliance.

The USA PATRIOT Act is an Act of Congress signed into law by United States President George W. Bush on October 26, 2001, in response to the September 11 attacks. The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes, some of which include:

- To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism;

- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse;
- To require all appropriate elements of the financial services industry to report potential money laundering.

Below is a brief, non-comprehensive overview of the sections of the USA PATRIOT Act that may affect financial institutions.

- Section 311: Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern
- Section 312: Special Due Diligence for Correspondent Accounts and Private Banking Accounts
- Section 314: Cooperative Efforts to Deter Money Laundering
- Section 326: Verification of Identification. It prescribes regulations setting forth minimum standards for financial institutions that relate to the identification and verification of any person who applies to open an account
- Section 352: Anti-Money Laundering Programs
- Section 356: Reporting of Suspicious Activities by Securities Brokers and Dealers

Terminology and Acronyms

Money Laundering

We already provided the definition of money laundering given by the US Department of the Treasury. In short, it’s a process of hiding the origins or destination of the money by funneling it through a number of financial transactions. For example, drug dealers want to conceal the origin of their cash. On the other hand, some people or organizations may want to transfer legally obtained funds to finance terrorism.

Most criminals run their business in cash and try to make their payments (especially large ones) using cash. The US government passed laws that prohibit large payments in cash, which forces criminals to find ways to legitimize the sources of cash or "launder money". Producers who sell life insurance, often have to accept large amounts of money, which makes such financial products popular in the money laundering techniques.

Anti-money laundering

While criminals may be involved in money laundering, they are being confronted by government, law enforcement, business (i.e. insurance institutions). So AML is a set of procedures, regulations, and laws created to prevent a specific area of illegal activity - turning the dirty money into clean ones.

Financial institutions (e.g. insurance companies) have to investigate the customer prior to opening an account or selling a financial product. Some insurance agents might be willing to break rules to earn large commissions when a money launderer is willing to buy an expensive policy. AML procedures should prevent this from happening.

Know Your Customer

One of the AML procedures is called Know Your Customer (KYC). KYC is the process organizations use to verify, collect, and classify a customer's identity. This can be seen as a customer identification process where a customer's identity, financial status, and address are verified. This verification process must be carried out before financial institutions (e.g. banks or insurance carriers) can onboard customers and open new accounts. You can find more details about the identification and verification of any person who applies to open an account in section 326 in the USA PATRIOT act.

When deciding whether to do business with the potential client, the insurance company has to establish facts about the client and analyze his or her behavior. Can we verify that the clients are who they say they are? Do the facts they tell us to match what we could find from other sources? Have they interacted with similar firms before? Is their behavior or activity suspicious and requires reporting or investigation?

An insurance company needs to know its customers to comply with the relevant regulations and be reasonably certain that the prospect can become a client and receive insurance products. Typically, KYC controls include the following:

- Collection and analysis of basic identity information such as identity documents (e.g. driver license, passport, a national ID card)
- Name matching against lists of known parties (such as "politically exposed person")
- Determination of the customer's risk in terms of propensity to commit money laundering, terrorist finance, or identity theft
- Creation of an expectation of a customer's transactional behavior
- Monitoring of a customer's transactions against expected behavior and recorded profile as well as that of the customer's peers

Terrorist financing

The USA PATRIOT act is a more than 300-page document passed by the U.S. Congress with bipartisan support and signed into law by President George W. Bush on October 26, 2001, just weeks after the September 11 terrorist attacks against the United States. The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes, some of which include:

- To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism;
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse;
- To require all appropriate elements of the financial services industry to report potential money laundering;
- To strengthen measures to prevent the use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate the repatriation of stolen assets to the citizens of countries to whom such assets belong.

After the September 11 terrorist attacks, such government organizations as the Federal Bureau of Investigation and Treasury Department started to pay more attention to money laundering. The reason is that the laundered money was used for financing the preparation of the attack. While terrorists could use legal money as well, the laundered money represents a substantial share of funds used for preparing terror attacks.

Money transfers coming from certain countries may require special attention, and the Global Terrorism Index 2018 (see http://visionofhumanity.org/indexes/terrorism-index/) represents "a comprehensive study analyzing the impact of terrorism for 163 countries and which covers 99.7 percent of the world's population." Of particular interest are the sections covering the emerging hotspots of terrorism, as well as the drivers behind global terrorist recruitment.

OFAC

The Office of Foreign Assets Control (OFAC) of the US 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 US 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.

As part of its enforcement efforts, OFAC publishes a list 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. This information is publicly available at https://www.treasury.gov/resource-center/sanctions/sdn-list/pages/default.aspx.

When obtaining the credit report on a customer, see if it contains OFAC alerts. For recent OFAC actions visit the Web site of the US Department of the Treasury at https://www.treasury.gov/resource-center/sanctions/ofac-enforcement/pages/ofac-recent-actions.aspx.

FinCEN

Financial Crimes Enforcement Network (FinCEN) was created in 1990 to support federal, state, local, and international law enforcement by analyzing the information required under the BSA, one of the nation's most important tools in the fight against money laundering. The BSA's recordkeeping and reporting requirements establish a financial trail for investigators to follow as they track criminals, their activities and their assets.

FinCEN researches and analyzes this information and other critical forms of intelligence to support financial criminal investigations. The ability to link to a variety of databases provides FinCEN with one of the largest repositories of information available to law enforcement in the country. Safeguarding the privacy of the data it collects is an overriding responsibility of the agency and its

employees-a responsibility that strongly imprints all of its data management functions, and indeed, all that the agency does.

For more information about FinCEN see https://www.fincen.gov.

FATF

Financial Action Task Force (FATF) is an inter-governmental body that sets standards and promotes effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is, therefore, a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF has developed a series of recommendations that are recognized as the international standard for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

SAR

The Suspicious Activity Report (SAR) is a tool provided under the BSA for monitoring suspicious activities that would not ordinarily be flagged under other reports (such as the currency transaction report). Suspicious Activity Reports can cover almost any activity that is out of the ordinary. An activity may be included in the Suspicious Activity Report if the activity gives rise to a suspicion that the account holder is attempting to hide something or make an illegal transaction.

SARs are used to prevent and report the activities that seem to be related to money laundering. These reports can generate leads for law enforcement agencies. The insurance broker notifies the insurance carrier when suspicious activity occurs. Insurance carriers file SARs with FinCEN.

Willful Blindness

In AML efforts, *willful blindness* means not questioning a transaction when one suspects that something is amiss. The motivation of insurance agents to engage in willful blindness would usually relate to being paid a commission on the transaction if it is executed. To protect themselves from charges of willful blindness, agents have to report any suspicious activity to the AML compliance officer and retain a copy of the information for their records.

AML and SAR for insurance companies

FinCEN regulations impose AML compliance program requirements and SAR obligations only on insurance companies; there are no independent obligations for brokers and agents. However, the insurance company is responsible for the conduct and effectiveness of its AML compliance

program, which includes agent and broker activities. The insurance regulations only apply to a limited range of products that may pose a higher risk of abuse by money launderers and terrorist financiers.

Money launderers and terrorist organizations have considerable knowledge of life insurance companies and intermediaries and take extreme measures to hide their financial activities and make them indistinguishable from legitimate transactions. A risk-based approach in creating the AML compliance program is designed to make it more difficult for these criminal elements to make use of life insurance companies and intermediaries due to the increased focus on the identified higher risk activities that are being undertaken by these criminal elements.

In addition, a risk-based approach allows life insurance companies and intermediaries to more efficiently and effectively adjust and adapt as new money laundering and terrorist financing methods are identified.

According to the BSA/AML Examination Manual published by the Federal Financial Institutions Examination Council, a covered product, for the purposes of an AML compliance program includes:

- A permanent life insurance policy, other than a group life insurance policy
- Any annuity contract, other than a group annuity contract
- Any other insurance product with features of cash value or investment

Each of the above products has a cash value that can be transferred, and these products fall into AML regulations. On the other hand, there are products with a low risk of money laundering (e.g health or term life insurance), and they are exempt from the AML procedures.

Banks often engage in insurance sales to their customers, and in such sales, the insurance company may rely on the bank's AML 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 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 on the common activity with the insurance company.

The stages of money laundering

The money laundering is a process that can be broken down into three stages:

1. Placement - depositing illicit cash into banks or other financial institutions
2. Layering - a number of complex transactions (e.g transferring money between bank accounts in different countries) so the money appears legal.
3. Integration - the criminal uses the money that comes from various legitimate sources.

Placement

During the placement stage, the criminal wants to get rid of cash by placing it into a legitimate financial system. Imagine a drug dealer who needs to get a large sum of smaller currency bills into

a banking system. During this stage, money launderers are the most vulnerable to being caught because a customer that brings a large amount of cash always raises a red flag to the workers of a bank.

The criminals can use a technique called smurf - breaking up a transaction involving a large amount of money into smaller transactions below the reporting threshold.

For any transaction exceeding $10,000 in cash, a US business or financial institution must file a currency transaction report (CTR) by filing the IRS form 8300. Therefore, a criminal group with $50,000 in cash may use several smurfs for depositing anywhere from $5,000 to $9,000 in a number of accounts geographically dispersed.

Layering

After the placement stage comes layering (a.k.a. structuring). This is the most complex stage and often includes moving funds internationally. The main goal of this stage is to separate illicit money from its source.

The money can change accounts, ownership, type of financial products, countries et al. The money can go to shell companies (the fake ones), trusts, or real estate. The money can go through different jurisdictions to make them as hard to trace as possible.

The criminals may purchase several financial instruments that can subsequently be converted into clean money. For example, he can purchase several permanent life insurance policies (e.g. whole or universal life).

Integration

During this stage, the illicit money is being used with the appearance of legitimate funds by moving the money back into the legal monetary system. A criminal may invest the money into the business, or sell expensive items (e.g. houses and yachts) bought during the layering stage.

If the money launderer managed to buy a permanent life insurance policy, he can borrow the money against this policy's cash value or even surrender the policy (or annuities), and the check arrives from the insurance company.

If the goal of money laundering was terrorist financing, during the integration phase, the money will be distributed to terrorist organizations.

Review questions

1. Insurance companies are required to file SAR with
    a. FBI
    b. IRS
    c. FATF
    d. FinCEN
2. Which of the following insurance products are not covered by AML regulations?

a. An annuity contract other than a group annuities contract
b. Whole life insurance
c. Universal life insurance
d. Term life insurance

3. A money launderer decides to borrow the money against the whole life insurance policy purchased with illicit funds. This is an illustration of which money laundering phase?
   a. Placement
   b. Layering
   c. Integration
   d. None of the above
4. A customer deposited $11,000 in cash into his bank account. The bank must file the following:
   a. CTR
   b. SAR
   c. Both
   d. None of the above
5. A customer deposited $50,000 in cash into his bank account during the same day from multiple branches. The bank must file the following:
   a. CTR
   b. SAR
   c. Both
   d. None of the above
6. A customer bought ten whole life insurance policies and five annuity contracts over the past year using money orders and traveler's cheques. Which phases of money laundering this activity could represent?
   a. Placement
   b. Layering
   c. Integration
   d. None of the above
7. Which of the following statements is correct?
   a. AML regulations apply to all US-based insurers
   b. AML regulations apply only to insurers engaged within the US as a business in the issuing or underwriting of covered products.

Part 2 Responsibilities of producers and agencies

Insurance products that have cash value can be used in money laundering. For example, currency can be used to purchase one or more life insurance policies, which may subsequently be quickly canceled (surrendered) by a policyholder for a fee. The insurance company refunds the money to the purchaser by sending a check, and the criminals may be willing to pay the surrender fees to get clean money.

Even if the insurance policy doesn't have a cash value, there is a chance that it can be used to launder money or finance terrorism through the submission by a policyholder of false claims to its insurance carrier, which if paid, would allow the insured to recover a part or all of the originally invested payments.

The ways insurance products can be used to launder money include:

- Borrowing against the cash and surrendering value of permanent life insurance policies.
- Selling units in investment-linked products (such as annuities).
- Using insurance proceeds from an early policy surrender to purchase other financial assets.
- Buying policies that allow the transfer of beneficial interests without the knowledge and consent of the issuer (e.g. second-hand funding).
- Purchasing insurance products through unusual methods such as currency or currency equivalents (e.g. money orders).
- Buying products with insurance termination features without concern for the product investment performance.

To mitigate money laundering risks, *insurance companies* have to adopt policies, procedures, and processes that include the identification of higher-risk accounts and customer due diligence. *Insurance agencies* should review early policy terminations report the unusual and suspicious transactions (e.g. a large premium payment in cash, early redemptions with payments to apparently unrelated third parties and loans against the policy).

On November 3, 2005, FinCEN published rules specifically for insurance carriers:

- Insurance companies have to develop and implement AML programs
- Insurance companies must report suspicious transactions

These AML programs must be risk-based, i.e. account for specific risks the insurer faces. In the insurance industry, AML programs are geared specifically to preventing money laundering using *covered products*, for instance:

- An permanent life insurance policy, other than a group life insurance policy;
- An annuity contract, other than a group annuity contract;
- Any other insurance product with cash value or investment features.

The definition incorporates a functional approach and encompasses any insurance product having the same kinds of features that make permanent life insurance and annuity products more at risk of being used for money laundering, e.g., having a cash value or investment feature.

Producers contact new customers first and they are uniquely positioned to detect the first signs of illegal activities. This even includes the applicant's manner in answering application questions. Producers must be alert for circumstances that don't quite make sense and ask follow-up questions to verify customer answers that seem unclear or unusual and be prepared to decline applications from persons who will not or cannot comply with requests for identifying information.

Producers should keep notes of all conversations and observations and report all red flags to their managers or field compliance principals as directed by the company's AML process. The producer should not discuss any suspicion with the customer nor should the producer contact federal authorities directly.

AML regulations only apply to insurance carriers but exclude agents and brokers. However, carriers are held responsible for compliance with their AML programs, which include the activities of any agents and brokers. That's why carriers require brokers and agents to complete AML training and apply acquired knowledge in their daily activities. The carrier's AML program must include the following:

- A designated compliance officer responsible for implementing the program
- Ongoing training of appropriate persons, including insurance agents and brokers
- Policies, procedures and internal controls customized to the AML risks of the firm
- Ongoing compliance monitoring, including testing for compliance of insurance agents and brokers

In addition to AML Programs, carriers are required to submit suspicious activity reports described in Part 3.

An insurance agency, like any business in the US, has a legal obligation to report the receipt of more than $10,000 in cash or cash equivalents.

Insurance carriers are expected to use their contractual relationships to require agents and brokers to provide them with information that may be useful for identifying potentially suspicious activity.

Carriers have numerous compliance and best practices guidelines (including AML) that both captive and independent agents and brokers follow in order to continue doing business with them.

Insurance companies and their agents and brokers take serious efforts to prevent, identify, and report suspicious financial transactions. Insurance carriers, brokers, and agents make it difficult for criminals to use insurance products for illegal purposes, which strengthens the life insurance industry and the economy in which it operates.

Review questions

1. Which of the following statements is not correct?
    a. Money laundering is used to hide the origin of funds.

b. A large portion of funds used in terrorist financing comes from money laundering.

c. Insurance companies must monitor transactions for suspicious activity possibly related to money laundering.

d. Insurance agencies must monitor transactions for suspicious activity possibly related to terrorist financing.

2. Which organization published the rules obligating insurance carriers to create AML programs?

   a. FINRA

   b. LIMRA

   c. FinCEN

   d. FATF

3. An insurance agency receives the payment from a customer in the amount of $10,500 in the form of money orders and traveler's checks. Does this transaction have to be reported to the IRS?

   a. Yes

   b. No

4. Do AML regulations apply to general agencies?

   a. Yes

   b. No

   c. Only if the agency is large

5. Do insurance carriers require that only captive agents complete the AML training or it applies to the independent agents as well?

   a. Only captive agents

   b. Only independent agents

   c. Both captive and independent agents

6. Can insurance carriers use their contractual relationships to require agents and brokers to provide them with information about the suspicious activity?

   a. Yes

   b. No

Part 3 Suspicious activity reporting

Reporting

In May 2006, it became mandatory for insurance companies to file suspicious activity reports regarding some covered products. SARs can cover almost any unusual activity that gives rise to a suspicion that the account holder is attempting to hide something or make an illegal transaction.

Insurance company filers most commonly cited “BSA/Money Laundering/Structuring” as the characterization of suspicious activity. Structuring, where larger transactions are broken into smaller exchanges, is consistent with an attempt to avoid currency reporting requirements.

Say a money launderer has $200,000 in cash that he wants to get into the financial system. This amount would be a subject of a currency transaction report, so he or a group of smurfs can make 20-25 deposits to the same account on the same day using different bank branches or ATMs at different times. The financial institution would still file the CTR but also would also file a SAR.

A determination as to whether a SAR must be filed should be based on all the facts and circumstances relating to the transaction and the client in question. Different types of clients and transactions will require different judgments. Some of the red flags that may require SAR include the following:

- Application for a policy from a potential client in a distant place where a comparable policy could be provided “closer to home”
- Introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organized criminal activities or corruption are prevalent
- An atypical incidence of pre-payment of insurance premiums insurance policies with premiums that exceed the client’s apparent means
- Insurance policies with values that appear to be inconsistent with the client’s insurance needs
- Any transaction involving an undisclosed party
- Early termination of a product, especially at a loss, or where cash was tendered and/or the refund check is to a third party
- A client exhibits an unusual concern regarding the insurer’s compliance with government reporting requirements or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents
- Substitution, during the life of an insurance contract, of the ultimate beneficiary with a person without any apparent connection with the policyholder
- Requests for a large purchase of a lump sum contract where the policyholder has usually made small, regular payments
- The applicant for insurance business shows no concern for the performance of the policy but much interest in the early cancellation of the contract
- The applicant for insurance business attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by checks or other payment instruments

- The applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency
- A client appears to be acting as the agent for another entity but declines evades, or is reluctant to provide any information in response to questions about that entity.

This list is not complete because the techniques of money laundering or terrorist financing are continually evolving, and there is no way to provide a definitive list of suspicious transactions.

SAR completion and filing are a critical part of the SAR monitoring and reporting process. Appropriate policies, procedures, and processes should be in place to ensure SARs are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing. Insurance company file the "SAR-IC" report (form 108) with FinCEN.

Financial institutions should report the information that they know, or that otherwise arises, as part of their case reviews. SAR narratives should make available clear, concise and invaluable information to law enforcement investigators.

A FinCEN SAR shall be filed no later than 30 calendar days after the date of the initial detection. If no suspect is identified on the date of such initial detection, an insurer may delay filing a FinCEN SAR for an additional 30 calendar days to identify a suspect, but in no case shall reporting be delayed more than 60 calendar days after the date of such initial detection.

A continuing report should be filed on suspicious activity that continues after an initial FinCEN SAR is filed. Insurers may file SARs for continuing activity after a 90-day review with the filing deadline being 120 days after the date of the previously related SAR filing. Insurers may also file SARs on continuing activity earlier than the 120-day deadline if the institution believes the activity warrants earlier review by law enforcement.

A FinCEN SAR and any information that would reveal the existence of the FinCEN SAR are confidential and may not be disclosed except as specified in FinCEN’s regulations. On the other hand, a financial institution that has filed a SAR may share it or any information that would reveal the existence of the SAR, with an affiliate, provided the affiliate is subject to a SAR regulation.

Under federal law, insurance agents and brokers, as well as insurance companies, are protected from liability to customers for disclosing possible criminal activity to their insurance companies, law enforcement, and certain government supervisory agencies. SARs and the fact that they have been filed must be kept confidential. Customers cannot be notified that suspicious activity has been reported.

An insurer has to retain all filed SAR-IC reports for at least 5 years, but insurers usually retain records as long as there is a financial relationship with the customer and 5 years beyond the termination of the financial relationships. The insurance agent should keep copies of any customer information sent to the AML compliance officer.

FinCEN defines $5,000 as the suspicious activity review threshold amount. Any covered product transaction that includes a payment (or aggregate of payments) of $5,000 or more requires a closer evaluation by the insurer to assess the need to file a SAR-IC.

This doesn’t mean that all transactions exceeding the $5,000 threshold must be reported to FinCEN,

but such transactions should be closely reviewed by the carrier's AML compliance committee. Similarly, suspicious transactions below the $5,000 threshold may and should be reported.

Penalties

Penalties for money laundering by organizations and individuals fall into three categories:

1. Criminal
    - Fines in dollar amounts or as a multiple of the property involved in the transaction - whichever is greater
    - Prison sentences
2. Civil
    - Fines in dollar amounts or the value of funds involved in the transaction - whichever is greater
    - Seizure of any property involved
3. Reputation
    - Damage to the insurance company's reputation
    - Damage to personal and professional reputation

Criminal penalties for money laundering and terrorist financing can be severe. A person convicted of money laundering can face up to 20 years in prison and a fine of up to $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both (see Title 18 US Code § 1956).

Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property, and, under certain conditions, entire financial accounts (even if some of the money in the account is legitimate), may be subject to forfeiture. Pursuant to various statutes, financial institutions and individuals may incur criminal and civil liability for violating AML and terrorist financing laws.

The U.S. Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions. There are criminal penalties for willful violations of the BSA and its implementing regulations under 31 USC 5322 and for structuring transactions to evade BSA reporting requirements under 31 USC 5324(d).

For example, a person, including a financial institution employee, willfully violating the BSA or its implementing regulations is subject to a criminal fine of up to $250,000 or five years in prison, or both. A person who commits such a violation while violating another U.S. law, or engaging in a pattern of criminal activity, is subject to a fine of up to $500,000 or ten years in prison, or both.

The federal banking agencies and FinCEN have the authority to bring civil money penalty actions for BSA violations, and they make annual adjustments to the amounts of civil monetary penalties. IRS maintains a web page with a breakdown of criminal penalties for violation of BSA.

Financial institutions may be fined for violating AML program requirements. For example, FinCEN issued an assessment order against UBS Financial in the amount of $14.5 million for willfully

violating AML requirements. Aegis Capital assessed $1.3 million for SAR filing failures.

Moreover, compliance executives of a financial institution can be penalized personally, as it happened with Thomas E. Haider, the former Chief Compliance Officer of Moneygram in 2017. He agreed to pay a $250K penalty for his company AML failures. This was a settlement amount; FinCEN wanted to impose a $1M penalty.

But even if a financial institution or its executive has no problem paying these penalties, the reputational damage rapidly exceeds the fine once the institution's non-compliance becomes public.

The reputation of any business is essential to its survival. The trust and confidence of the consumer can have a direct and profound effect on a company's bottom line. Loss of reputation is a big risk for any brand, potentially costing future business. The same holds true for a professional, e.g. an insurance producer or an executive. For example, besides paying the penalty, the former COO of Moneygram was barred from working as a compliance officer for any money transmitter for three years.

If an insurance firm violates the AML program requirements, it can result in the loss of reputation, which in turn may cause a fall in stock prices and loss of customers and profits.

Criminal and civil penalties exist for violations of any regulations administered by OFAC. The penalties can be levied against the institution as well as the individuals involved. Criminal penalties include a fine of up to $1M and/or up to 20 years in prison for each violation.

Civil penalties include a fine of up to $55,000 for each violation. Other penalties for violations of OFAC regulations include the denial of export privileges and seizure/forfeiture of the goods involved.

Strictly following AML regulations will further reduce the susceptibility of insurance firms to being used by individuals or organizations to launder funds and fight terrorist financing, thereby reducing their exposure to damage to their reputation, a key asset in the financial services industry.

Review questions

1. Are insurance agents contractually obligated to report suspicious activity?
    a. Only captive agents
    b. All insurance agents
    c. Only if the agency is large
2. Which form insurance companies use to file the SAR report?
    a. SAR-INS, form 108
    b. SAR-IC, form 108
    c. SAR-SF, form 101
    d. SAR-INS, form 101a
3. Which of the following statements are correct?

a. Independent insurance agents are required to file SARs
b. Insurance agents are required to file SARs if they work for an agency
c. Insurance agents are expected to work with carriers in identifying suspicious transactions that the carrier must report
d. If an agent suspects there is a potential for money laundering they should immediately contact the carrier's AML compliance officer and await instructions.

4. A financial institution can't delay reporting after the date of initial detection
    a. more than 90 calendar days
    b. more than 60 calendar days
    c. more than 30 calendar days
5. Why some insurers may keep SAR records for more than 5 years?
    a. Because the AML regulation may change in the future
    b. Because it doesn't cost much to keep SAR longer
    c. Because the insurer may still have financial relations with the customer but initial detection happened more than 5 years ago
6. Can customers sue an insurance company or an agent for disclosing their possible criminal activity?
    a. Certain states allow this
    b. Yes
    c. No
7. What kind of penalties can an insurance company face for not reporting suspicious activity related to money laundering?
    a. Criminal charges
    b. Civil charges
8. Does the amount of penalties and the length of imprisonment for money laundering increases if a person also violated other US laws ?
    a. Yes
    b. No
9. Which of the following penalties can be imposed for each OFAC violation?
    a. Fine of up to $1M and/or up to 20 years in prison
    b. Fine of up to $500K and/or up to 10 years in prison
    c. Fine of up to $250K and/or up to 5 years in prison

Answers to Review Questions

Part 1

1. d)
2. d)
3. c)
4. a)
5. c)
6. b)
7. b)

Part 2

1. d)
2. c)
3. a)
4. b)
5. c)
6. a)

Part 3

1. b)
2. b)
3. c) and d)
4. b)
5. c)
6. c)
7. b)
8. a)
9. a)