Amalgamated Life
Life • Accident • Disability

Dear Agents/Brokers,

Amalgamated Life Insurance Company is responsible for ensuring that all appropriate persons receive training on money laundering prevention on a regular basis; fully understand relevant anti-money laundering procedures and their importance; and understand the ramifications for noncompliance.

Federal regulations require insurance companies to train their insurance producers and brokers regarding their responsibilities in terms of anti-money laundering including identifying suspicious customer behavior and transactions as well as procedures to report suspicious activities. An ongoing training program is a core element of the anti-money laundering regulations.

Amalgamated Life Insurance Company is ultimately responsible for monitoring the effectiveness of its training program and assuring compliance with these regulations. The following section outlines the Amalgamated Life Insurance Company Anti-Money Laundering program.

For further questions regarding the Amalgamated Life Anti-Money Laundering (AML) Training, please contact our legal department at (914) 367-5941.

Thank you,
Amalgamated Life Insurance Company
333 Westchester Avenue
White Plains, NY 10604
914-367-5000

Amalgamated Life
Life • Accident • Disability

POLICY STATEMENT

Amalgamated Life Insurance Company is committed to preserve the financial integrity and reputation of both our company and our agents/brokers. We want to ensure that the purchase of our products is not used in any scheme to launder money that might in turn be used to support illegal activities including, but not limited to: organized crime, drug trafficking, and terrorism. We have developed this short course of training to advise our agents and brokers how to spot potential money laundering schemes, to take steps to avoid becoming unwitting participants in them, and where to report any suspicious activity.

Amalgamated does not, and will never, knowingly participate in money-laundering activities with any individual or business. We will promptly report all suspicious activities to the relevant agencies, and cooperate in any resulting government investigation. Any employee or contractor who is found to have participated in money laundering or other criminal activities, or to have willfully failed to report suspicious activities as required by this document will be subject to disciplinary action, up to and including termination of employment or contract, as well as civil or criminal prosecution.

After you have reviewed the contents of the training material, please return the certification that located at the end of the material, attesting that you have completed your review. We will keep the certification in your permanent file.

TRAINING OBJECTIVE

This document is intended to provide a brief overview of money laundering schemes and the ways in which the insurance industry might be used to further such illicit activities. In addition, this policy provides an overview of the requirements imposed by the US Treasury Department and similar regulatory bodies.

Amalgamated is ultimately responsible for the conduct and effectiveness of our anti-money laundering program, which includes monitoring the activities of the agents and brokers that work with covered products. However, we recognize the crucial role that our agents and brokers play, due to their direct contact with our customers, in protecting Amalgamated, our employees, third party vendors and clients from being targeted for money laundering schemes, terrorist financing, or other financial crimes.

Through this training, Amalgamated seeks to integrate our agents and brokers into our anti-money laundering program, and to advise them of the ways in which we will monitor compliance with the program. The standards set forth in this document represent the minimum requirements based on applicable laws and regulations, and apply to all activities of Amalgamated Life Insurance Company.

WHAT IS MONEY LAUNDERING?

Money laundering is the process in which assets obtained through illegal activities are invested or transferred into legitimate channels, to give the appearance that the funds are from legal sources. The original, illegal source of the funds is obscured in a way that makes their origin difficult or impossible to trace. Dirty money is essentially "washed clean" by conversion into seemingly legitimate assets. Money laundering is a very complex crime involving intricate details, numerous financial transactions and financial outlets throughout the world. The US has a large, complex and open financial system, which makes it a target for illicit activity.

Businesses can become unwitting participants in money laundering schemes, because the source of funds used to purchase their products, goods or services is unknown to them. Federal Law makes it illegal for financial institutions, including insurance companies, to engage in money laundering, and requires that reasonable steps be taken to avoid involvement in such schemes.

The 3 Stages of Money Laundering

Money Laundering, although a single process, tends to have three distinct stages, which are discussed in detail below:

1. Placement

The “placement” stage represents the initial entry of the "dirty" cash or assets into the financial system, in small amounts. This stage serves two purposes: (a) it relieves the criminal of the burden of carrying and guarding large amounts of cash; and (b) it places the money into the financial system via legitimate financial vehicles.

Placement can be accomplished in a number of ways. The launderer could employ a number of individuals (“smurfs”) to deposit small amounts of illicit money (generally less than $10,000) into bank accounts for transfer in the near future, in order to defeat bank threshold reporting threshold requirements. Brokers can be used structure large deposits of cash in ways that disguise the original source of the funds. Illicit money can be used to establish businesses that act as “fronts” in which illicit money can be blended with legitimate funds. Other common methods of placement include loan repayment, gambling, and currency exchanges.

Money launderers are the most vulnerable to being caught during the placement stage. This is due to the fact that placing large amounts of cash into the legitimate financial system can take time and raise suspicions.

2. Layering

The "layering" stage is meant to obscure the link between the illicit money and its source by moving funds around via complex financial transactions that make it difficult for law enforcement to trace back to their origin. There are several methods of layering. Cash that has been "placed" may be converted into monetary instruments, such as money orders, bank drafts, travelers' checks, and gift cards. Cash might be used to purchase tangible assets such as cars, jewelry, art work, and homes that can be resold. Money might also be moved or transferred through numerous accounts. All of these methods seek to make it harder for law enforcement to trace funds back to their source, and make it easier for launderers to evade detection.

3. Integration

The final stage of the money laundering process is the "integration stage", in which the laundered funds are moved back into the economy from seemingly legitimate sources. Once fully "integrated" into the financial system, the funds can be used for any purpose. There are many different ways in which the laundered money can be integrated. "Front" companies can be used to make apparent purchases of goods and services from co-conspirators, or to issue fake loans to such individuals from what appear to be legitimate business proceeds. Tangible property purchased during the layering stage can be unloaded for profit. .

Money launders have been known to purchase products such as whole life and other types of policies that build up cash value because they can cash them in early, in exchange for fees that are negligible compared to the funds that they can legitimize through the transaction. Launderers may also purchase insurance for seemingly legitimate business reasons and then repeatedly make overpayments of premiums in order to obtain refunds of the "mistaken" overpayments as a means to launder money.

Money Laundering "Red Flags"

Below are some of the most common "red flags," which should raise suspicion, and prompt subsequent action, including further investigation and in some cases, the reporting of the activities to the relevant authorities:

- Clients who provide false, misleading or substantially incorrect information concerning the source of funds used to purchase a product, or who either fail to indicate or refuse to identify a legitimate source of funds.

- Clients who exhibit a lack of concern for the costs associated with the purchase of a covered product, but seem overly focused on early termination features (free -look period), or withdrawal or loan features.

- Clients who purchase multiple policies with different insureds, particularly where there appears to be no legitimate personal or business reason. Clients that maintain multiple policies under a single name.

- Sales with a premium paid by a third party or through a premium financing arrangement.

- Products for which beneficiaries appear unrelated to the owner or are located overseas.

- The business involves non-U.S. persons, foreign bank accounts, governments or government officials, or jurisdictions subject to Office of Foreign Assets Control sanctions (currently, the Balkans, Belarus, Burundi, Central African Republic, Cuba, Darfur, Republic of the Congo, Iran, Iraq, Lebanon, Libya, North Korea, Somalia, (South) Sudan, Syria, Ukraine, Venezuela, Yemen and Zimbabwe).

Other signs of Money Laundering

a. *Customers who Provide Insufficient or Suspicious Information*
- Providing unusual or suspicious identification documents that cannot be readily verified.
- Reluctance to provide complete information about the nature and purpose of a business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Refusal to identify a legitimate source for funds or provide information that is false, misleading or substantially incorrect.
- Having a background that is questionable or that differs from general expectations based on business activities.

b. *Efforts to Avoid Reporting and Recordkeeping Requirements*
- Reluctance to provide information needed to file reports or failure to proceed with a transaction.
- Attempts to persuade an employee/broker/agent not to file required reports or not to maintain required records.
- "Structured" deposits, withdrawals or purchase of monetary instruments below a certain dollar amount to avoid reporting or recordkeeping requirements.
- Seeming overly concerned with the firm's compliance with government reporting requirements and the firm's AML policies
- Reluctance to provide information needed to file reports or failing to proceed with a transaction

c. *Transactions Involving Insurance Products*
- Client cancels an insurance contract and directs funds to a third party.
- Rapid withdrawal of funds shortly after a deposit of a large insurance check when the purpose of the fund withdrawal cannot be determined.
- Cancelling annuity products within the free look period which. Although such activity could be legitimate, it may signal laundering of funds if accompanied with other suspicious actions.
- Opening and closing accounts with one insurance company then shortly thereafter reopening a new account with the same insurance company, each time with new ownership information.
- Purchasing an insurance product with no concern for investment objective or performance.
- Purchasing an insurance product with unknown or unverifiable sources of funds, such as cash, official checks or sequentially numbered money orders.

d. Activity Inconsistent With Business
- Transactions patterns show a sudden change inconsistent with normal activities.
- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.
- Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.
- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

e. Other Suspicious Customer Activity
- Receipt of law enforcement subpoenas seeking information on the customer.
- Large numbers of securities transactions across a number of jurisdictions.
- Payment by third-party check or money transfer without an apparent connection to the customer.
- Payments to third-parties without apparent connection to customer.
- No concern regarding the cost of transactions or fees (*i.e.*, surrender fees, higher than necessary commissions, etc.).

APPLICABILITY OF AML REGULATIONS TO INSURANCE

An insurance company is defined as a "financial institution" under the Bank Secrecy Act (defined in the next section). The term "insurance company" and "insurer" is defined in Treasury regulations implemented as a result of the PATRIOT Act as any person engaged within the US as a business in the issuing or underwriting of "covered products." Covered products are those insurance products that have been determined to present a higher degree of risk for money laundering:

- Permanent life insurance, other than group life insurance
- Annuity contracts, other than a group annuity contract
- Any other insurance product with features of cash value or investment

Because they pose a lower risk for money laundering, the following products are not deemed to be covered products:

- Group insurance products
- Term (including credit) life, property, casualty, health or title insurance
- Reinsurance and retrocession contracts
- Contracts of indemnity and structured settlements, including workers compensation payments

The limiting definition is meant to incorporate a functional approach, and encompasses any insurance product having the same kinds of features that place permanent life insurance and annuity products at higher risk of being used for money laundering schemes, *e.g.* having a cash value or investment feature. To the extent that term life insurance, property and casualty insurance, health insurance, and other kinds of insurance do not exhibit these features, they are not deemed to be products covered by the rule. If an insurance company that is not presently issuing or underwriting a covered product should do so in the future, the insurance company would become subject to the rule, to the extent of its business relating to covered products.

AML OVERSIGHT AND ENFORCEMENT

Most AML regulations, oversight, and administrative enforcement activities fall within the jurisdiction of the US Department of the Treasury, although the Internal Revenue Service and Securities and Exchange Commission also play limited roles. The sections below provide an overview of the regulations that govern money laundering, as well as the agencies that enforce them.

Applicable Laws*:*

Bank Secrecy Act

The Bank Secrecy Act (BSA) was passed by Congress in 1970 as one of the first anti-money laundering laws in the United States. The BSA established requirements for recordkeeping by private individuals, banks and other financial institutions in order to help identify the source, volume, and movement of currency and other monetary instruments that are transported or transmitted into or out of the United States or deposited in US financial institutions. These records are used by law enforcement agents, both domestically and internationally, to identify, detect and deter money laundering whether in furtherance of a criminal enterprise, terrorism, tax evasion, or other unlawful activity.

Money Laundering Control Act

The Money Laundering Control Act of 1986 established money laundering as a federal crime, prohibited structuring transactions to evade Currency Transaction Report filings, introduced civil and criminal forfeiture for BSA violations, and directed banks to establish and maintain procedures to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA.

USA PATRIOT Act

The USA PATRIOT Act was enacted on October 26, 2001, in response to the September 11, 2001 terrorist attacks. The PATRIOT Act established a host of new measures to prevent, detect and prosecute those involved in money laundering and terrorist financing activities. Title III of the PATRIOT Act, (also referred to as the "Money Laundering Abatement Act"), added new anti-money laundering provisions and amendments to the BSA in an effort to make it easier for authorities to prevent, detect, and prosecute money laundering and the financing of terrorism. These amendments:

- Expanded the anti-money laundering program requirements to all financial institutions, including insurance companies
- Increased civil and criminal penalties for money laundering
- Provided the Secretary of the Treasury with the authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money laundering concern"
- Criminalized the financing of terrorism and augmented the existing BSA framework by strengthening customer identification procedures

- Improved information sharing between financial institutions and the U.S. government by requiring government-institution information sharing and voluntary information sharing among financial institutions

The PATRIOT Act requires financial institutions, including insurance companies to establish AML programs, related due diligence policies, procedures, and controls reasonably designed to detect and report money laundering, that comply with regulatory standards developed by the Treasury Department and its Financial Crimes Enforcement Network (*discussed in the next section)*.

AML Oversight Agencies:

US Treasury Department

The US Department of Treasury (US Treasury) is the agency that primarily oversees and enforces anti-money laundering regulations. The Treasury promotes economic prosperity and ensures the financial security of the United States by operating and maintaining systems that are critical to the nation's financial infrastructure, such as the production of coin and currency, the disbursement of payments to the American public, revenue collection, and the borrowing of funds necessary to run the federal government. The Treasury works with other federal agencies, international financial institutions and foreign governments, and performs a critical and far-reaching role in enhancing national security by implementing economic sanctions against foreign threats to the US, identifying and targeting the financial support networks of national security threats, and improving the safeguards of US financial systems.

Financial Crimes Enforcement Network - FinCEN

The Financial Crimes Enforcement Network (FinCEN) is a bureau within the US Treasury that collects and analyzes information about financial transactions in order to combat domestic and international money laundering, terrorist financing, and other financial crimes. The PATRIOT Act required the Treasury to create a secure network for the transmission of information to enforce the relevant AML regulations. FinCEN's receives requests from federal law enforcement agencies, and sends bi-weekly data requests to more than 45,000 points of contact at more than 27,000 financial institutions, which must conduct data matches of accounts and transactions of persons that may be involved in terrorist financing and/or money laundering. The partnership between the financial community and law enforcement allows investigators to canvas the nation's financial institutions for potential "leads" into laundering schemes that might otherwise never be discovered.

Office of Foreign Assets Control - OFAC

The Office of Foreign Assets Control (OFAC) is a financial intelligence and enforcement agency within the U.S. Treasury that is charged with the planning and execution of economic and trade sanctions in support of U.S. national security and foreign policy objectives. The Patriot Act requires that all persons and businesses doing business in the U.S. comply with OFAC regulations.

OFAC maintains a list of countries, organizations, and individuals with whom U.S. organizations are prohibited from conducting business unless specifically authorized by OFAC. These lists are regularly updated and should be cross-checked against a company's transactions. Compliance with OFAC regulations requires checking the names of new customers or parties to a new transaction against the existing Specially Designated Nationals (SDN) list and screening existing customers or counterparties database against updates to the list. All matches, or "hits" must be investigated and cleared before a transaction can be completed and before reporting to OFAC.

OFAC is empowered to levy significant penalties against entities that defy it, including imposing colossal fines, freezing assets, and altogether barring parties from operating in the United States. There are severe fines and legal actions that the U.S. Treasury can take against organizations that either knowingly or negligently fails to check the OFAC Anti-Money Laundering blacklists before making payments or engaging in business transactions.

New York State Department of Financial Services - NYSDFS

The Department of Financial Services (NYSDFS), regulates the financial services and insurance industries at the state level. NYSDFS deems compliance with the BSA/AML and OFAC monitoring and reporting requirements to be essential to prudent risk management. NYSDFS reserves the right to make inquiry into a licensee's compliance function in order to assess how well the licensee contemplates the risks of money laundering, bribery of foreign persons, and recognition of federal economic sanctions.

The review will be conducted within the overall review of a company's overall compliance function during periodic audit examinations.

AML Regulatory Reporting:

Suspicious activities and resulting investigations must be reported to regulatory agencies within days of the initial detection of facts that may constitute a basis for its reporting. Both the FinCEN Suspicious Activity Report (SAR) and federally mandated OFAC regulations are discussed below.

Suspicious Activity Reports:

Insurance companies that issue or underwrite "covered products" are required to report suspicious transactions to FinCEN in the form of a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR). The criteria for determining when a report must be made varies, but the requirement is, generally, any financial transaction that does not make sense to the financial institution, that is unusual for that particular client, or that appears to be done only for the purpose of hiding or obfuscating a transaction. All of the facts and circumstances relating to a transaction and the customer affecting it should be evaluated in determining whether or not a transaction is suspicious and, therefore, whether a report should be filed. Though the SAR Rule does not provide specific criteria, the aforementioned "red flags" serve as examples of potentially suspicious transactions.

Agents and brokers are most likely to identify transactions that may be suspicious, on the basis of their direct customer contact. Suspicious activity must be promptly reported to Amalgamated's Compliance Officer, who is responsible for the day-to-day operation of Amalgamated's AML program. The Compliance Officer will review the information provided, and determine whether a report by Amalgamated is warranted. The agent or broker must not at any point inform either the client or the parties to the suspicious transaction that a SAR is being contemplated or has been filed.

SAR reports must be made to FinCEN within 30 business days. Insurance companies must maintain copies of the reports and the original or business record equivalent of any supporting documentation for five years after filing the report. The threshold amount for reporting a suspicious transaction is $5,000 in funds or other assets, determined by either the premium payment or the potential payout, regardless of whether such amounts involve currency.

Note: A current version of the SAR can be found on the FinCEN website. FinCEN is actively engaged in the development of a web based Suspicious Activity Report filing system useable by all program participants and accessible with only an internet connection and browser.

OFAC Reporting:

Companies must report transactions that are blocked or rejected on the basis of OFAC matches within ten business days from the date of disposition. OFAC requires the retention of all reports and blocked or rejected transaction records for at least five years, for purposes of ascertaining compliance with OFAC regulations. Additionally, US financial firms are required to file annual reports of all property blocked as of June 30, of each year, due by September 30.

AML REGULATORY ENFORCEMENT

As stated in the previous section, the US Treasury is the agency that primarily oversees and administratively enforces US anti-money laundering regulations. AML enforcement authority generally lies within FinCEN, as the agency that is responsible for investigating suspected violations of the AML Rules and imposing civil penalties for identified violations. Additionally, OFAC imposes restrictions on financial institutions, which must take actions to either reject or block prohibited transactions involving sanctioned persons or governments. Both AML and OFAC require the identification of suspicious financial transactions and reporting to the U.S. government.

In recent years it has been common for the U.S. government to bring enforcement actions that involve violations of both AML and OFAC regulations. For this reason, many financial institutions implement both AML and OFAC responsibilities together

PENALTIES

Money laundering is a federal crime, which means that penalties are articulated in the United States Code, and are subject to sentencing schedules. Charges are investigated and brought by the Department of Justice.

Laundering of Monetary Instruments: (18 USC § 1956)

Imposes a fine of the greater of $500,000 or twice the value of the property involved in a transaction, imprisonment of up to 20 years, or both for persons who know, or have reason to know that property involved in a financial transaction represents the proceeds of some form of unlawful activity, and who either conduct or attempt to conduct a transaction involving such proceeds where the person knows that the transaction is designed, in whole or in part (i) to conceal or disguise the nature, location, source, ownership, or control of the proceeds, or (ii) to avoid a transaction reporting requirement under state or federal law. There is also a potential civil penalty of up to the greater of $10,000 or the value of the property involved in the transaction.

Engaging in Monetary Transactions in Property Derived From Specified Unlawful Activity (18 USC § 1957)

Persons that knowingly engage or attempt to engage in a monetary transaction involving criminally derived property of a value greater than $10,000 are subject to a fine, imprisonment for up to ten years, or both.

OFAC Penalties

Violations of OFAC can result in penalties of up to $1,000,000 and 12 years in jail per violation. There is no "safe harbor" under OFAC, however, violations will be reviewed based on the overall circumstance. Factors such as the quality of the organization's compliance program, and voluntary disclosure can sometimes be deemed mitigating factors.

TIPS FOR AVOIDING MONEY LAUNDERING SCHEMES

1. *Know Your Customer*

The first step to avoiding involvement in money laundering schemes is to know your purchaser. Amalgamated Life Insurance agents and employees are the company's first line of defense, as they make direct contact with potential customers and are often in the best position to assess the customer, the nature of the customer's businesses, the objectives for which the insurance products are being purchased, and the financing contemplated for the transaction. Brokers and agents can be the eyes and ears of Amalgamated in obtaining a 'first impression' of the customer, as they engage in conversations with the customer and learn enough about the customer to assess whether a contemplated purchase makes sense for the purchaser.

Aside from anti-money laundering concerns, this is simply good business practice. You should be aware of transactions that require heightened security (as highlighted in the Red Flags section), be on the lookout for anything that seems to be inconsistent with the purchaser's best insurance purchasing and maintenance goals, and report any suspicions to Compliance.

2. *Verify Identity*

Based on the risk level, and to the extent reasonable and practicable, the identity of customers should be verified, and the accuracy of the information obtained from potential customers. A purchaser's identity must be verified by using both documentary and non-documentary means.

Documents should be the primary means to verify customer identity when appropriate documents are available. Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

- For a business entity, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

In verifying the customer's information, the identifying information received, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, (including EIN and TIN) should be used to assess whether the true identity of the customer has been provided (*e.g.*, whether the information is logical or contains inconsistencies).

Non-documentary means should be used, where there are unresolved questions concerning the identity of the customer after reviewing documentation. This includes instances when: the customer is unable to present an unexpired government-issued identification document with a photograph; the firm is unfamiliar with the documents the customer presents for identification verification; the customer and firm do not have face-to-face contact; and any other circumstances that increase the risk that the firm will be unable to verify the true identity of the customer through documentary means.

If your purchaser cannot produce satisfactory documentary proof of identity, other means of verifying their identity must be pursued. These may include:

- Reviewing credit bureau reports or Accurint.
- Checking the Secretary of State, Corporate Listings for the state in which the customer is incorporated.
- By visiting the business address, or checking Google Maps, to make sure the business is actually located there.
- Checking the internet for the customer's website, customer reviews, and independent listings of personnel, telephone numbers and other contact information provided by the purchaser to verify its existence.
- By checking references with other businesses or financial institutions.

The need to verify the customer's identity is heightened for certain types of accounts, such as those opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by OFAC as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. Added scrutiny should be given for these customers and their intended purchases.

Amalgamated will ultimately determine whether the information obtained is sufficient to form a reasonable belief that the true identity of the customer is known (*e.g.*, whether the information is logical or contains inconsistencies), and will maintain copies of documentation used to make this determination for at least five years.

3. *Adequate Record Retention*

All application materials should be well-documented, including copies of all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. Records should contain a description of any document relied on to verify the customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. Records should also be kept that reflect the method and amount of product payments.

With respect to non-documentary verification, records should be retained that describe the methods and the results of any additional measures taken, beyond documentation review, to verify the identity of a customer. Records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information should also be maintained. These records should be retained for at least five years after the record has been made or the account has been closed.

REPORTING SUSPICIOUS ACTIVITY

If you believe that an activity seems suspicious or falls outside of a normal range of activity for a particular purchaser or type of purchaser you must promptly report your suspicions to Amalgamated's Compliance Officer. The report can be made via the compliance line at (914) 367-5941 or anonymously at (866) 835-7650. You must not at any point inform the purchaser of your suspicions or that you have reported your suspicions to our Compliance Officer. Under the direction of the Compliance Officer, Amalgamated will determine whether to further investigate the matter, and if reporting to a regulatory agency is warranted.

The only exception to this reporting requirement is an instance in which the potential violation implicates the Compliance Officer, in which case the employee shall report the incident to Internal Audit. Such reports will be confidential, and the employee will suffer no retaliation for making them.

AMALGAMATED LIFE INSURANCE COMPANY

Thank you for participating in the Amalgamated Life Insurance Company Anti-Money Laundering Training. Please note that this document is an **internal training manual**.

If you produce business through another carrier, you may be required to take another course outside the Amalgamated Life Insurance Company Training process.

Please sign and return the enclose certification that says you have read these materials.

Amalgamated Life
Life • Accident • Disability

QUESTIONS

The following questions will assess your understanding of the materials.

1. Who is ultimately responsible for the conduct and effectiveness of the Amalgamated AML Compliance Program?

a. Amalgamated Life Insurance

b. Brokers and Agents

c. FinCEN

d. All of the above

2. Which of the following is NOT a stage of Money Laundering?

a. Placement of cash into the financial system

b. Layering multiple transactions

c. Inflating to increase the amount of funds

d. Integrating money back into the economy

3. Which insurance product is considered high risk for AML purposes?

a. Term life insurance

b. Reinsurance

c. Group annuity coverage

d. Permanent life insurance

4. Which was the first anti-money laundering law in the United States?

a. USA PATRIOT Act

b. Money Laundering Control Act

c. Bank Secrecy Act

d. Foreign Assets Control Act

5. What changes did the Patriot Act make with respect to Money Laundering Requirements?

a. Increased civil and criminal penalties for money laundering

b. Criminalized the financing of terrorism

c. Expanded anti-money laundering requirements to insurance companies

d. All of the above

6. What does it mean if a customer appears on the OFAC list?

a. Amalgamated cannot do business with the customer under any circumstances

b. Amalgamated must obtain permission from OFAC to proceed with the transaction

c. The OFAC list has no effect on the ability of Amalgamated to proceed with a business transaction

d. A report should be made to the Federal Bureau of Investigations

7. How many days after detection should a Suspicious Activity Report be filed with FinCEN?

a. 10

b. 30

c. 90

d. 365

8. At what point should a customer be made aware that a Suspicious Activity Report is contemplated:

a. At the point that the suspicions arise

b. During the Compliance Investigation

c. After the report is made to FinCEN

d. The customer should never be made aware

9. Which is a method of verifying a corporation's identity?

a. Reviewing certified articles of incorporation

b. Checking the Secretary of State, corporate listings

c. Reviewing a government-issued business license

d. All of the above

10. What violation carries the highest penalty?

a. Laundering of Monetary Instruments

b. Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity

c. Violations of Office of Foreign Assets Control requirements

d. All of the penalties are the same

11. What steps can be taken to avoid involvement in monetary schemes?

a. Get to Know Your Customer

b. Verify the Customer's Identity

c. Retain Adequate Records of a Transaction

d. All of the above

12. Which of the following is <u>not</u> a red flag that a customer may be involved in money laundering?

a. Client cancels an insurance contract and directs funds to a third party.

b. Threats to murder the policyholder

c. Attempts to persuade an employee/broker/agent not to file required reports or not to maintain required records.

d. Providing information that is false, misleading or substantially incorrect.

Amalgamated Life
Life • Accident • Disability

CERTIFICATION

I have received a copy and read the Amalgamated Life Insurance Anti-Money Laundering Training Manual. I acknowledge that I am now fully aware of the Company's policy in this regard, and the procedures for reporting suspicious activities.

I further acknowledge that I can be subject to discipline, up to and including termination of employment or contract for violating this policy.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

OFFICE USE ONLY
Compliance Signature:
Date: