Anti-Money Laundering Training

Brought to you by:
National Guardian Life Insurance Company

Course Objectives

The objective of this training course is to ensure you have the knowledge to detect and prevent money laundering.

After completing this course, you will be able to:

- Protect yourself from involvement in anti-money laundering activities
- Understand how anti-money laundering works
- Recognize the red flags associated with it
- Understand the Know Your Customer requirements and how they apply to the insurance business

Overview

The USA Patriot Act (the "Act") was enacted by the U.S. Congress and signed into law on October 26, 2001. The name of the Act is an acronym for Uniting and Strengthening America ("USA") by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("PATRIOT"). This broad-sweeping legislation is intended to aid in the war against terrorism.

The Act does the following things:

- Strengthens U.S. anti- money laundering laws;
- Enhances criminal and civil penalties for violations;
- Grants new powers and surveillance capabilities to law enforcement agencies.

Anti-money laundering laws in the United States are enforced primarily by the Federal Reserve Board and the Treasury Department. The Treasury Department's enforcement is through an internal office known as the Financial Crimes Enforcement Network (FinCen). Its mandate is to fight money laundering and financial crimes.

NGL supports the intent and spirit of the USA Patriot Act and in particular its anti-money laundering and anti-terrorism initiatives. All NGL employees and agents are encouraged and expected to attain an appropriate level of familiarity with:

- The USA Patriot Act and its provisions addressing anti- money laundering and the reporting of suspicious activities
- An understanding of the procedures adopted by NGL to assure compliance with the Act
- An appropriate level of expertise to accomplish the purpose of our procedures and the Act's intent.

Lesson One: What is Anti-Money Laundering?

Money Laundering

The criminal practice of filtering illegally obtained money through a series of transactions to "clean" the funds so that they appear to be proceeds from legitimate activities.

Although this practice is typically tied to cash, any financial transaction may be a part of a process to filter the money. Non-cash transactions often play a significant role in money-laundering activities.

The Three Stages of Money Laundering

Money laundering typically follows three stages (also known as mechanics):

1. Placement
2. Layering
3. Integration

* These three stages can occur individually or simultaneously.*

Stage One: Placement

Placement is the first stage of money laundering by which money from criminal activity is placed in a financial institution. A common method of placement is Structuring, which is breaking up currency transactions into portions that fall below a reporting threshold in an effort to avoid reporting or record keeping requirements.

Example: *A client deposits $50,000 cash via several transactions of $10,000 or less into a money market account.*

Stage Two: Layering

Layering is the process of conducting a complex series of financial transactions, with the purpose of hiding the origin of money from criminal activity and hindering any attempt to trace the funds. This stage can consist of multiple securities trades, purchases of financial products including life insurance or annuities, cash transfers, currency exchanges, or purchases of legitimate businesses.

Example: *The client now has $50,000 in a money market account. First he writes a check for $20,000 in order to purchase a whole life insurance policy. Secondly he writes a check for the remaining $30,000 to be deposited into an annuity with another carrier.*

Stage Three: Integration

The final stage is Integration in which legitimate transactions are used to return the now-laundered funds back to the criminal.

Example: *The client cancels the insurance transactions during the free-look period and accepts returned funds, minus any appropriate surrender charges and fees.*

Ramifications and Penalties of Money Laundering

- Fines can be up to twice the amount of the transaction, up to $1 million.
- Any property involved in the transactions may be subject to seizure
- Employees of financial institutions can be fined individually and sentenced up to 20 years incarceration for knowing or being willfully blind to the fact that the transaction involved illegal funds.
- To avoid potential charges always report any suspicious behavior to NGL's Compliance Officer and keep documentation of those reports.
- Anyone who does not comply with NGL's policies and procedures is subject to disciplinary action up to and including termination of appointment or employment and will be reported to the proper legal authorities.

Lesson Two: Know Your Customer

Lesson Overview

This section will identify the Know Your Customer procedures used to collect required information about our customers.

NGL agents and employees are in direct contact with customers and are often in a critical position of knowledge as to the source of investment assets, the nature of the clients, and the objectives for which the insurance products are being purchased. These individuals and entities have an important role to play in assisting NGL in the prevention of money laundering and in the identification of suspicious transactions.

Following these procedures will help decrease the chance that NGL will be used to facilitate money laundering activities. It will also help you understand your customer's financial goals.

Develop a Customer Profile

Developing a customer profile provides the ability to:

- Identify appropriate transactions
- Determine whether a pattern exists which is inconsistent with a customer's goals and business
- Determine which activities may require further investigation

Under the Know Your Customer requirements you must make reasonable efforts to:

- Collect identifying information about the customer,
- Verify the information, and
- Learn enough about the customer's financial picture and goals to determine whether a transaction makes sense for that customer.

Why You Need to Know Your Customer

The financial information that you need to gather for Know Your Customer purposes is information you would normally collect as part of a needs analysis. The more you know the better you can service your customers.

The majority of clients are not involved in money laundering activities, so it is important to be able to distinguish routine from suspicious transactions.

Verifying an Individual's Identity

There are four primary pieces of information needed to verify a customer's identity (there may be additional information needed based on a company's requirements):

- Name
- Address
- Date of Birth
- Social Security or Tax Identification Number

Acceptable Identification

The easiest way to verify an individual's identity is through a government issued identification card such as:

- Driver's license
- U.S. passport
- U.S. Military card
- State photo ID card
- Resident alien ID card (green card)
- Foreign government ID card (resident or non-resident aliens)

Verifying Customer Identity

The USA Patriot Act requires that the customer be notified that the carrier must verify the identity of the owner of any policy or account. This can be accomplished by filling out a USA Patriot Act Notification and Customer Identification Verification form and having it placed in the client's file.

While you will not be required to make a photocopy of the ID card, you should physically look at it and copy down the identification number on the card. You should also confirm that the information on the card is consistent with other information you have about the customer's identity.

There may be times when physically seeing an individual's identification is not possible, such as when you are doing business via telephone, through the mail or online. NGL will determine when non-documentary methods should be used and will typically conduct the verification. This may include:

- Comparing the information included on an application or service request form against a third party resource such as Accurint or a fraud detection service
- Contacting the customer to verify information given
- Checking other financial institutions

There may be instances in which additional review is necessary by a carrier before a policy can be issued or an account opened.

Official Resources

There are two agencies who are involved in specialized due diligence and enhanced scrutiny over certain individuals:

Office of Foreign Assets Control (OFAC)

This group maintains a list of specially designated nationals and blocked persons (SDNs). These individuals are deemed to be a threat to national security. Financial institutions are typically prohibited from conducting transactions with target countries, their nationals and SDNs . NGL has procedures in place to check customers against the OFAC list. Based on the findings you may be asked to obtain additional information in order to properly identify an individual and prevent any false-positive reporting.

Financial Action Task Force (FATF)

This group maintains a list and conducts a periodic review of non-cooperative countries. These countries have serious deficiencies in their anti-money laundering rules and regulations which may attract money laundering activities. Financial institutions can do business in these countries but must exercise enhanced due diligence.

Record Retention

Regulations require that information related to customer identification be:

- Kept for a minimum of five years, and
- Be reasonably accessible to regulators

Be sure to file any customer information you obtain in your client's file along with any information you have provided to NGL. Always remember that your responsibility does not end at the point of sale. Report any suspicious requests or interactions from the customer to NGL for further review.

Again, knowing your customer is the most important deterrent to money laundering.

Lesson Three: Suspicious Activity and Red Flags

What constitutes a suspicious activity?

This will depend on your clients and the normal course of their business. If anything seems out of line or suspicious it is worth further review. Things to look for include:

- Payments to or from unknown third parties
- A drastic change in business patterns
- High number of cash or currency transactions
- Incomplete information provided with no level of detail
- Requests for early termination of insurance policies without concern over surrender charges or penalties.

Reporting Illegal Activities

Whenever you suspect or know that a transaction involves funds related to illegal activity you must report the transaction to NGL's Compliance Officer.

As part of this process you must NOT notify the client that their business activities have been or may be reported as suspicious, are under investigation, or that a Suspicious Activity Report (SAR) has been filed.

Notification of the client is prohibited by federal statute.

Red Flags

The following is a listing of potential red flags in various situations:

New Accounts:

- Application for a policy in a distant place even though the client could get a comparable policy closer to home.
- Application for coverage is outside the client's normal pattern of purchases.
- Client unwilling to provide identity verification documentation
- Applicant reluctant to provide normal personal information
- Applicant uses a mailing address outside of regulator's authority
- Applicant's telephone number found to be disconnected when attempting to verify information

Transactional Red Flags

- Any transaction involving an undisclosed third party
- Requests for a large purchase of a lump-sum contract where the policyholder's experience is typically regular payment, small face amount contracts, unless there are appropriate reasons.
- 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.
- Applicant for insurance business requests to make a lump- sum payment by a wire transfer or with foreign currency.
- Applicant for insurance business establishes a large insurance policy, and within a short time period cancels the policy and requests the cash value returned, payable to a third party.
- Applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.

Other Red Flags

- Transfers of the benefit of a product to an apparently unrelated third party
- Multiple changes of address or changes of owners to foreign countries
- Attempts to use a third party check to make a proposed purchase of a policy.
- Applicants with no concern for the performance of the policy but much concern for the early cancellation.
- Applicants who buy policies from several institutions in a short time frame.
- Applicants purchasing policies in amounts considered beyond the client's apparent means or needs.
- Large overpayments of premiums.
- Unusually great concern with the insurer's or your own compliance with reporting requirements.

Business Areas

The Treasury Department has identified certain types of businesses that lend themselves to money laundering and warrant increased scrutiny. The following are examples of the types of businesses which should raise red flags for potential involvement in money- laundering activities:

- Casinos and other gambling establishments
- Offshore corporations and banks or businesses located in high-risk foreign countries
- Travel agencies
- Used automobile dealers and machine parts manufacturers
- Import/export companies
- Jewel, gem and precious metal dealers
- Pawnbrokers and deposit brokers
- Check-cashing facilities
- Money transmitters
- Currency exchange houses

Money Laundering Through the Insurance Industry

The information below demonstrates how individuals launder funds through the insurance industry based on the type of products used. This may include:

- Permanent Life Insurance
- Variable Annuities
- Overpayment of Premiums
- Wires

Permanent Life Insurance

This type of insurance is attractive to a criminal, as this type of product builds cash value which is available as a withdrawal or loan.

For example, a client purchases a large single premium policy and then cancels the policy. The fees and penalties are worth the price compared to the amount of funds they are able to access. A money launderer expects to lose a small percentage of their funds in this process.

Variable Annuities
An individual wishing to launder funds may purchase a variable annuity and then cancel the contract during the free-look period. This way they have managed to receive a check from a legitimate source without paying any fees or penalties.

An individual may also withdraw money from an annuity regardless of any fees or penalties which are considered part of the process.

Overpayment of Premiums
A money launderer may arrange for insurance coverage of his or her legitimate business then repeatedly over pay the premiums. They then call the carrier and claim to have accidentally overpaid and request a refund of the overage. The result is that they have a check from a reputable source.

Wires
While not a common method of funding an insurance policy, criminals may launder illegal funds through excessive numbers of transfers for
high dollar amounts.

Compliance Officers Contact Information

Primary Contacts	
Kimberly Shaul, Senior Compliance Officer	608-443-5219 kashaul@nglic.com
Michael Lowe, Senior Compliance Officer	276-645-4303 mlowe@settlerslife.com
Additional Contacts	
Jerie Olson	608-443-5244 jaolson@nglic.com
Carolyn Arnold	276-645-4313 carnold@settlerslife.com