Financial Crime Training for Producers

Anti-Money Laundering and Fraud

2020

Financial Crime Training

Introduction/Objectives

Global Atlantic FINANCIAL GROUP

Introduction

As a regulated financial institution, Global Atlantic is subject to anti-money laundering (AML) laws and regulations, in accordance with the USA PATRIOT Act, that requires the company to have policies, procedures, and controls to prevent and detect money laundering, insurance and securities fraud, identity theft, terrorist financing, bribery, and other illegal activity. The penalties associated with failure to identify or report suspicious activity can be severe.

As an agent of Global Atlantic, you are the first line of defense against the company being a victim of or used to facilitate illegal activities. You are responsible for being alert and escalating suspicious activity to protect yourself and the company from potential reputational, financial, and legal harm.

Objectives

By the end of this training you will be able to:

- Define the key elements of financial crime as they relate to money laundering and fraud
- Understand the responsibility of agents to prevent, detect, and escalate suspicious activity
- Be familiar with sanctions regulations
- Identify red flags for potential suspicious activity
- Understand the role of the Special Investigation Unit (SIU) and know where to report suspicious activity

Financial Crime Training

Fraud

Global Atlantic does not support and will not knowingly assist in any activity that facilitates fraud. It is Global Atlantic's policy to comply with all laws, regulations, and company guidelines that apply to the business of the company and to, wherever possible, prevent the occurrence of fraudulent activities.

As with money laundering, failure to adhere to regulatory and company requirements may lead to disciplinary action, up to and including termination of your appointment with any Global Atlantic insurance company subsidiary.

What is fraud?

Fraud is the intentional act of deception, misrepresentation, impropriety or concealment to gain something of value to the detriment of another. This includes the manipulation of records to disguise the true components of a transaction.

Key types of fraud that will be focused on are:

1. Identity
2. Employee
3. Customer Account
4. Vendor/Supplier
5. Customer/Application
6. Claim
7. Elder Exploitation

Global Atlantic FINANCIAL GROUP

Identity Theft

Identity theft is the unauthorized use of an individual's personal identifying information, such as name, taxpayer identification number or account number, in order to commit fraud or other crimes.

- Examples and Red Flags for Identity theft include but are not limited to the following:
  - A customer is unwilling to provide basic/required information to open an account
  - The customer is only available via cell phone or a non-office number
  - Personal identifying information provided is inconsistent when compared against external information sources
  - The address, phone number, or social security number is the same or similar to that of several others opening accounts or other existing accounts
  - A customer purports to represent a company but provides only general generic information about the entity and cannot provide evidence of ongoing and legitimate business activity
  - Third parties are being involved in an account opening process without evidence of acting under appropriate authority (i.e. a trading authorization, management agreement or other)
  - The customer expresses an extreme sense of urgency to complete a transaction

Customer Account Fraud

Common indicators of potential fraud associated with a customer account are:

- Premium payments from agents or clients of agents
  - Multiple accounts are used to pay premiums
  - Attempted use of cash for payments
- Fraudulent or fictitious applications
  - Fictitious applicants or insured's, hence why Know Your Customer is important
  - Attempt to gain coverage normally unattainable
- Use of misleading practices
  - Product, coverage, or premium amounts are falsified in advertising
  - Use of deceptive advertising
- Forgery with or without intent
  - More and more states are deeming forgery a felony with possible imprisonment
- Misappropriation of funds
  - Individuals not associated with a policy withdrawing funds
  - Premiums not applied to the policy as instructed by the policyowner

Customer/Application Fraud

Application fraud is often the result of misrepresentations in the application. Agents should be familiar with these common misrepresentations and pay close attention to any potential red flags related to the customer providing this information.

Examples of the types of information misrepresented in an application are:

- Age
- Identity (fraudulent documentation)
- Reason for purchasing the product
- Medical condition or history

Misrepresentation can be prevented by:

- Asking all health questions to the proposed insured.
- Provide additional clarifying information regarding various health conditions
- Record the proposed insured's responses truthfully and completely on the application
- Validation of personal documentation (Know Your Customer)
- Document any observations related to health and mortality you make during the application process

Claim Fraud

Claim Fraud is a prime target for fraudulent activity.

Potential indicators of claim fraud are:

- Altered or fictitious documents supporting death
- Elaborate schemes to stage or fake death
- Requesting a sharp increase in coverage prior to a claim
- Frequent questions about a claim just prior to requesting a claim be processed
- The policy is in effect a short time before a claim, or the claim is made just prior to the lapse/expiration of the policy
- Payments to or by unknown third parties
- Death allegedly occurs outside of the United States (especially in less developed or emerging countries) and supporting documentation (e.g., proof of death, proper identification) is suspicious
- Death of the insured occurs shortly after a policy is purchased, contestable period expires, existing policy amounts are increased or reinstated, or multiple policies are purchased
- Backdating of premium payment or application to predate death

Ways to protect the company from being a victim of claim fraud are:

- Obtaining a ‘certified’ death certificate or a statement from the U.S. Embassy for International deaths.
- Use of online obituaries in conjunction with other documents when fraud is suspected
- Utilize external sources where possible, such as a death index or Accurint
- Review policy documents carefully along with the claim documentation looking for any red flags

Elder Abuse, Exploitation and Diminished Capacity – Background

- Older adults (typically 60 years or older) can be exceptionally vulnerable to abuse and financial exploitation by any person or caregiver close to them.
- Elder financial exploitation refers to the act or process of taking advantage of an elderly person by another person or caretaker whether for monetary, personal or other benefit, gain or profit. Elder financial exploitation is rising dramatically with Federal and state regulators paying increasing attention to the issue.
- Life events, such as the death of a spouse, may lead to an unprepared change in management of an older adult's finances. Older adults are potential victims of financial exploitation regardless of income level.
- It is important to use special care when working with elderly customers. Trust your instinct and escalate any concerns to your manager. Please become familiar with both behavioral and financial Red Flags of elder abuse and elder financial exploitation.
- Diminished capacity is also something you should be aware of as it can lead to elder abuse and exploitation.
- Similar vigilance for financial abuse Red Flags should also be used for any other adult who may have a mental or physical impairment that renders the individual unable to protect his or her own interests.
- It is imperative that the individual customer's privacy is protected and their integrity is respected. Any suspected exploitation must be reported in good faith and with reasonable care.

If you suspect or have concerns that financial exploitation may be occurring, please contact Global Atlantic's Compliance Department at fraud@gafg.com.

Red Flags of Elder Abuse, Exploitation, and Diminished Capacity

- Older adult lacks knowledge about personal financial status
- Noticeable change in banking or financial management habits (such as more frequent or larger withdrawals or activity)
- New inability to afford the cost of daily living
- Unusual degree of fear, anxiety, submissiveness or deference during interactions
- Sudden appearance of previously uninvolved relatives claiming their rights and/or facilitating financial transactions on behalf of the older adult
- Excessive interest in older adult's finances or accounts is expressed by trusted others
- Unable to hold a prolonged conversation
- Seem confused or disoriented or is unable to keep up with current events.
- Uncharacteristic nonpayment for services
- Disregard to penalties
- Change of address to a new address
- Suspicious signatures
- Abrupt changes to financial documents such as power of attorney, joint accounts, account beneficiaries
- Making requests beyond legal authority outlined in provided documents
- Funds are not being used in the interest or intent of the older adult
- Provides contradictory or questionable explanations for transactions
- More than one person is claiming legal authority for the customer

Global Atlantic FINANCIAL GROUP

What is Money Laundering?

Money laundering is a complex process involving three different and sometimes overlapping phases:

1. *Placement* – Placement removes illegal cash from the location of acquisition to avoid detection from the authorities and transforms it into a legitimate form such as traveler's checks, money orders, or deposits into financial institutions.
2. *Layering – Separates illegally obtained money from its source by 'layering' it through a series of transactions. For example transferring funds into several different financial institutions to conceal the source and ownership of the funds. Layering makes it difficult to trace funds back to the original source.*
3. *Integration – Integration moves the assets into a legitimate form. Layered funds are used to purchase legitimate products or services to fund criminal and illegitimate activity. The launderer's goal is to integrate the 'cleaned' money into the economy.*

Money laundering in the insurance industry is accomplished in the layering and integration phases.

- The purchase of a life insurance policy contract with illicit funds allows a money launderer to integrate the funds into the economy as legitimate.
- The payment of premiums via wire transfer and through various accounts can be an example of Layering.

Global Atlantic approaches money laundering by addressing three key components:

1. **Prevention**
2. **Detection**
3. **Escalation**

It is critical that each of the components be performed and properly documented to protect the company.

1. Prevention

Prevention begins at the start of a relationship with any customer, be it an agent, policy owner, vendor or a potential business partner. This is the best time to safeguard the company from suspicious activity as you will be obtaining information that could be indicative of suspicious activity.

Due diligence, often known as 'know your customer' (KYC) is required at the beginning of any relationship. The scope of the due diligence may vary depending on the type of customer (i.e. employee, vendor, agent, counterparty, customer, agency, etc.)

There are three basic questions that must be answered and documented at the onset of any relationship to help identify customers with a high money laundering risk.

These questions are:

1. Who is the customer?
2. What is the nature of the business?
3. What is the source of the customer's wealth/assets?

As part of the KYC process you must collect basic information about the customer, also known as the Customer Identification Program (CIP).

The CIP requires the company to collect, among other things:

- Information regarding the customer's ownership and control
- Verification of the identity of the customer
- Record and retain the customer identification and verification information

If a potential customer fails, or is unable to provide verifying information or documents, or if the information provided appears questionable, the company may decide not to conduct business with the potential customer.

The company also needs to ensure that no current or potential customer, counterparty, or related person is named on any sanctioned list published by the Office of Foreign Assets Control (OFAC) or in a prohibited jurisdiction.

2. Detection

Being familiar with red flags for money laundering is the key to a company detecting potential money laundering or suspicious activity. Red flags are often related to recognizable inconsistent and/or suspicious behaviors as noted in the red flags below and identified in the Know Your Customer process explained on the previous page.

Red Flags

- Application contains incomplete information and client is excessively secretive, implying or suggesting that they do not want their identity revealed to regulatory authorities.
- Excessive cash or currency transactions
- Payments to or by unknown third parties
- Transactions involving an undisclosed party
- Borrowing the maximum cash value of a single premium policy after paying for it
- Changes of address or ownership to foreign country
- Transaction varies from the normal course of business for a life insurance policy
- Transaction is inconsistent with a customer's known legitimate business or personal activity
- Large and/or frequent overpayments of premium
- Early surrender of policy without concern over high surrender charges
- The client and/or its principals are the subject of negative news reports
- Financial information provided is false or cannot be verified

3. Escalation

Escalation is required of all agents and requires accurate, complete, and timely reporting of any suspicious activity, or fraud concerns. Escalations should be directed to fraud@gafg.com.

All agents must report suspicious conduct to their manager who will refer it to the appropriate AML/SIU Compliance Officer of the Company. Timely escalation is critical because in certain circumstances the company may be required to report such activity to regulatory officials.

Under no circumstances should you inform a customer or third party that a review, investigation, or reporting is underway. This is considered 'tipping off' and is prohibited by federal law.

To minimize the risk of inadvertently tipping off a customer, you should report your suspicions internally, on a strictly 'need to know' basis.

Once you have referred suspicious activity to your manager, **DO NOT**:

- Disclose your referral to anyone other than those on a need to know basis
- Discuss your referral with outside contacts without permission from Compliance
- Disclose to the subject of the referral that a review is being conducted. (This is considered 'tipping off' and is prohibited)
- Disclose that the referral is the reason why a transaction has been delayed

Breach of any of these requirements could subject you to disciplinary action up to and including termination and expose the company to significant fines and/or penalties.

Global Atlantic FINANCIAL GROUP

Bribery

Laws in various countries prohibit bribery by a firm, its personnel or any agent or intermediary acting on the firm's behalf. Bribery includes offering, making, or receiving payments or providing or receiving goods or services for the purpose of gaining an improper competitive advantage or inducing or rewarding the improper performance of a relevant function or activity.

Global Atlantic prohibits its personnel or agents from directly or indirectly providing or offering anything of value to any government official, counterparty, or prospective counterparty to obtain or retain business or to gain an improper business advantage. This includes the following:

- Public officials; candidates for office
- Employees or officers of counterparties, clients or suppliers
- Any agent of the aforementioned parties
- Any other person with whom the company conducts or anticipates conducting business with

A 'bribe' may include anything of value, including:

- Cash and gifts
- Meals and entertainment
- Employment
- Political contributions and charitable donations

Reporting/Escalation

Escalation of potential suspicious activity does not automatically mean the customer is engaged in illegal activity but you MUST report your suspicions to your manager who will refer it to the appropriate Compliance Officer. Please email any concerns with suspicious activity to fraud@gafg.com.

Special Investigation Unit*

The Special Investigation Unit (SIU) is responsible for investigating suspected suspicious activity including AML and Fraud that may be identified via red flags or otherwise. As part of their investigation, the SIU maintains documented files of their reviews and if necessary may ask the reporting party for additional information as part of their investigation.

The SIU is also responsible for handling any regulatory reporting related to the suspicious activity. There are various regulatory requirements on the timing of reporting therefore it is essential that matters of concern be escalated immediately and additional information if requested be provided timely.

SIU personnel monitor information made available by the states and other industry organizations to stay current on new and emerging insurance fraud trends. These findings are made available to all SIU personnel for review and discussion. The SIU meets periodically to review trends and potential issues arising from recent investigations.

Global Atlantic FINANCIAL GROUP

Certification of Participation in Forethought Anti-Money Laundering Program

Forethought Life Insurance Company

Training Certification Acknowledgements for Producers

I CERTIFY that I have read and understand Forethought's Anti-Money Laundering Training and Guidelines.

I understand that my failure to follow the Guidelines could result in the termination of my appointment with Forethought.

I acknowledge that I must complete a refresher Anti-Money Laundering (AML) course every 2 years, based on a rolling 24-month period, in order to remain in compliance.

Agent Signature	Date (MM/DD/YYYY)
Agent Name (Printed)	Agent Number

This Certification can be submitted as follows:

U.S Mail
Forethought Life Insurance Company
C/O Licensing and Contracting
P.O. Box 216
Batesville, IN 47006

Via Fax:
Please fax to (800) 668-5072

Via Email:
Please email to PreneedLicensing@gafg.com