Midland National Life Insurance Company
North American Company for Life and Health Insurance

ANTI-MONEY LAUNDERING PROGRAM

Revision Date: 8/1/2019

This document is only for distribution to Midland National and North American employees and producers.

Table of Contents

I. Purpose

In response to the terrorist attacks of September 11, 2001, Congress enacted, and the President signed into law, the USA PATRIOT Act on October 26, 2001. Section 352 of the Act amended the Bank Secrecy Act ("BSA") to require all financial institutions, including insurance companies, to develop and implement anti-money laundering programs.

Midland National Life Insurance Company and North American Company for Life and Health Insurance (the "Company" or collectively the "Companies") are firmly committed to combating terrorist financing, money laundering and other financial crimes (collectively "money laundering") and to complying with the spirit as well as the letter of the USA PATRIOT Act (the "Act").

The Act and the regulations promulgated under the Act require the Company maintain an anti-money laundering program. To comply with its legal and regulatory requirements, and to ensure that the Company, its employees and appointed producers, do not engage or unknowingly assist others engaging in money laundering, The Companies have established this Anti-Money Laundering (AML) Program (the "Program").

II. Scope

All officers, employees, appointed producers, and Company business units, including the Sammons Annuity Group and Corporate Markets, are subject to and must comply fully with the Program.

III. Background

Money laundering is the process of converting criminal proceeds into legitimate assets in order to disguise the illegal origin of the criminal proceeds. Money laundering typically occurs in three stages:

- Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.
- At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate and obscure the money from its criminal origin.
- At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

IV. USA PATRIOT Act and Bank Secrecy Act

A. Civil and Criminal Penalties

The Act strengthened penalties for failure to comply with the BSA. In addition to sanctions, the Companies may decide to impose on employees or producers who fail to comply with this Program, a violation of U.S. money laundering laws may be punishable by both criminal and civil penalties, applied to both the Company and to the employee or producer. The potential penalties for money laundering are severe and may include lengthy imprisonment, fines and forfeiture of assets.

B. Reputational Harm

In addition to possible criminal and civil sanctions, the mere suggestion of money laundering carries potential risk to one of the most valuable assets of the Companies: their reputation. The business of the Companies depends on honesty and integrity and harm to our reputation will cause severe business damage.

V. AML Program

Protecting the Company against exploitation by money launderers and financiers of terrorism is the responsibility of every employee and producer. The involvement of an employee or appointed producer in any aspect of money laundering - even if unintentional or indirect - may result in serious civil and criminal penalties for the Company, the employee and producer in addition to causing significant damage to the Company's reputation.

Every employee and appointed producer selling, administering or servicing any covered product must become familiar with the Program.

A. AML Requirements for Insurance Companies

Federal AML requirements for insurance companies are codified in 31 CFR Chapter X, and include establishing an AML program which includes, at a minimum, the following elements:

1) Designate an AML Officer who is responsible for ensuring the Program is implemented effectively;

2) Using a risk-based methodology, develop, implement and maintain policies, procedures and internal controls designed to guard against money laundering through the Company and to integrate its producers into its anti-money laundering efforts;

3) Establish an ongoing AML training program for producers and for appropriate employees concerning their responsibilities under the program;

4) Independent testing to monitor the adequacy of the Company's AML program periodically; and

5) Obtain formal approval of the Program by the Board of Directors of the Companies or by senior management.

B. Covered Products

The AML rules for insurance companies apply to certain kinds of products. The "covered products" are viewed by federal regulators as having a higher risk for use by money launderers, and are defined as:

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

The Company has assessed the risk exposure of its covered products and has considered these risks in developing this Program. The Company will periodically reassess the risk

exposure of its covered products to ensure the Program continues to address the risk of money laundering at or through the Company. This assessment will be the responsibility of the AML Compliance Officer.

C. AML Compliance Officer

The Company has designated a qualified AML Compliance Officer for the purpose of the Program and this designation has been approved by the Board of Directors. The AML Compliance Officer is responsible for overseeing compliance with the Program and is the primary contact for money laundering issues with employees, producers, regulators, and law enforcement.

The AML Compliance Officer's responsibilities include:

1. Implementation and monitoring of the daily operations of the Program
2. Appropriate annual training of employees
3. Producers' compliance with the Company's Program, including training requirements
4. BSA recordkeeping and reporting obligations, including reviewing reports of suspicious activities and determining whether to file a Suspicious Activity Report (SAR) and filing of a Form 8300
5. Apprising senior management and the Board of Directors of AML issues and status at least annually.
6. Updates and maintenance of the Company's risk-based Program, including the policies, procedures and controls appropriate for the risk presented by the products, customers, geographies and producers of the Companies, as well as for changes to regulations under the Act.

D. Training

The AML Compliance Officer shall ensure that those key personnel and producers receive adequate training and information regarding typical money laundering schemes, the legal and regulatory framework relating to money laundering, the Program, the AML procedures, and their role and responsibility in the process. Delivery of this training may include computer-based modules, lectures, and memoranda, or a combination of these methods.

1. Training of Producers

Insurance companies are required to "integrate" producers into their anti-money laundering program and to monitor their compliance with the program. Education and training will be provided by the Financial Crimes Unit in conjunction with the Sales and Marketing areas. The Financial Crimes Unit will determine the third-party education products that will be accepted by the Companies.

Producers play an important role in helping to prevent money laundering because of their knowledge of the customers, including sources of investment assets and customer objectives in purchasing insurance products.

AML training is provided to all new producers at the time they are contracted and on a biennial basis thereafter. Producers must complete the Company AML training or an AML training course approved by the AML Officer. Producers will not be allowed to solicit covered products on behalf of the Companies until the AML training requirements have been satisfied.

2. Training of Employees

All Company personnel will receive AML training upon employment. All Company personnel involved in writing or processing of covered products and/or the handling of funds will receive additional training on a biennial basis.

E. Customer identification Program

The Company has adopted a Customer Identification Program ("CIP"). The CIP requires the collection of certain information from each customer:

Required Customer Information

The following information will be collected for owners, annuitants, and insured of all new insurance and annuity applications:

- Name
- Date of birth,
- Street Address (Physical Address)
- Identification number, which will be a social security number ("SSN") or taxpayer identification number ("TIN") for U.S. persons or entities,
- For non-U.S. persons or entities one or more of the following;
    a. Passport number and country of issuance, or
    b. Alien identification card number, or
    c. Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

F. Office of Foreign Assets Control

The Company's policy is to comply with all Office of Foreign Assets Control ("OFAC") sanctions. The United States Department of the Treasury's Office of Foreign Assets Control administers and enforces economic and trade sanctions against targeted countries and their agents, terrorist groups, and international narcotics traffickers.

All U.S. insurance companies and U.S. citizens and permanent resident aliens who are employees, officers or directors of U.S. or foreign insurance companies are subject to OFAC's jurisdiction and accountable for sanctions violations.

For all (1) new applications received and on a ongoing routine basis, (2) disbursements, (3) new producers appointed, (4) new employees and (5) vendors, the Company will check to ensure that a person or entity does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List ("SDN List") and also is not engaging in transactions with people or entities from, sanctioned countries and regions.

In the event of a potential match to the SDN List or other OFAC List, the Financial Crimes Unit will conduct a review of the information and determine whether the match is a false positive. Potential matches that cannot be ruled a false positive will be escalated to the AML Officer. The AML Officer will communicate next steps to the business and provide handling instructions.

True matches will be reported to OFAC by the AML Officer within 10 business days.

Questions concerning compliance with OFAC regulations should be directed to the AML Officer. The AML Officer will contact OFAC if necessary.

G. Suspicious Activity

An AML compliance program must include the ability to identify, monitor, escalate to senior management and report suspicious transactions. Insurance companies are required to report suspicious transactions involving a "covered product" totaling/aggregating $5,000 in funds or other assets if we “know, suspect, or have reason to suspect” that a transaction:

- Involves funds derived from illegal activity or is intended to hide funds derived from illegal activities
- Is designed to evade other reporting requirements (such as "structuring" large cash transactions into smaller amounts)
- Had no business or lawful purpose
- Involves the use of the Company to facilitate criminal activity

In addition, the Company must refuse to open an account or establish a relationship for a customer if:

- **It is determined that the customer presents an unacceptable risk of money laundering, terrorist financing or other financial crime**
- **The Company cannot reasonably satisfy itself that it knows the true identity of a customer through its CIP set forth in this document**

Suspicious activity applies not only to currency transactions, but could also involve assets of any type, including monetary instruments, wire transfers, cashier’s checks, money orders, travelers checks or securities of any kind. A transaction that has no business or apparent lawful purpose, or is not the sort in which the customer normally would be expected to engage, where the Company knows of no reasonable explanation for the transaction after examining the available facts, would also be a suspicious transaction. Analysis should be routinely performed to determine whether or not a particular transaction structure could involve one or more of the Red Flags or be a part of one or more Stages of Money Laundering.

Red Flags

Red Flags that signal possible money laundering include but are not limited to:

- The customer exhibits unusual concern regarding the Company’s compliance with government reporting requirements and the Company’s AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.

- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer’s stated business strategy.

- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the Company's policies relating to the deposit of cash and cash equivalents.

- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000.00 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (“FATF”).

- The customer’s account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

- The customer’s account shows numerous cash equivalent transactions aggregating to significant sums.

- The customer’s account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

- The customer’s account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.

- The customer’s account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.

- The customer requests that a transaction be processed in such a manner to avoid the firm’s normal documentation requirements.

- Attempt to borrow maximum cash value of a single premium policy soon after purchase

If the appointed producer:

- Exhibits a dramatic or unexpected increase in sales (particularly of single premium contacts)
- Has consistently high activity in single premium contracts in excess of company averages
- Exhibits a sudden change in activity.
- Requests client documentation be delivered to the agent

H. Reporting

1. SAR

The company is required to report all suspicious activities to FinCEN in the form of a Suspicious Activity Report ("SAR"). If you deem an activity suspicious, contact the AML Officer, who has responsibility for investigating and filing a SAR.

Confidentiality of Suspicious Activity Reports
SARs are confidential. Under no circumstances are you to disclose that a SAR has been filed, considered, or that you have been asked to assist in providing information regarding suspicious activity to anyone, including the party involved in the transaction that is the subject of the SAR.

Therefore, employees or agents who report a suspicious transaction are not allowed to notify any person(s) involved in the transaction (*i.e.,* the agent, Insured, Policy Owner, etc.) that it has been reported. SARs can only be disclosed to appropriate law enforcement and supervisory agencies.

2. Form 8300

The Internal Revenue Code and certain BSA provisions require filing of reports (Form 8300) relating to cash or cash equivalents in excess of $10,000 received in a trade or business either in a single transaction or related transactions. The filing must be completed within 15 days of the transaction.

"Cash" for purposes of Form 8300 filing requirements is defined to include not only currency, but also a cashier's check, bank draft, traveler's check, or money order having a face amount of not more than $10,000 received in any transaction in which the recipient knows that such instrument is being used in an attempt to avoid the reporting of the transaction.

In addition, the company will furnish a written statement to each person whose name is required to be included in the Form 8300. The statement will be provided by January 31 of the year following the transaction. This statement will include the name, address, contact person, and telephone number of the business filing Form 8300, the aggregate

amount of reportable cash the business was required to report to the IRS from the person receiving the statement, and that the business provided this information to the IRS.

I. Information Sharing

The Company shares information with other financial institutions in accordance with section 314(b) for purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain a policy or engage in a transaction. The Companies will register with FinCEN to facilitate appropriate information sharing. The AML Officer is the designated contact under the Act. The Companies employ strict procedures to ensure that only relevant information is shared and to ensure protection of the security and confidentiality of this information.

J. Law Enforcement Requests

Law enforcement may request data from the Financial Crimes Unit on clients and transactions as part of an investigation they are working on. Law enforcement requests and inquiries can be received by phone, mail, or in person. Law enforcement requests can also include grand jury subpoenas, National Security Letters (NSL), and section 314(a) requests. The Patriot Act gives the Government greater power to demand information and freeze resources in financial institutions. Insurance Companies are required to comply. It is important for the Company not only ensure compliance with legal obligations, but also as a means of minimizing the risk of civil and criminal penalties. Failure to appropriately handle a law enforcement request, such as a grand jury subpoena for a criminal investigation, (where the Company is simply a witness providing documents) can quickly turn the matter into an investigation of the financial institution for obstruction of justice. All AML law enforcement requests should be directed to the AML Officer, who will be responsible for responding to the request for information. The request will be treated confidentially and a SAR may be filed if applicable.

K. Record Retention

The Companies shall maintain, for a period of not less than five years, funds transfers of $3,000 or more, copies of AML records / communications, AML training materials, reports (SAR, 8300, OFAC Reports) filed with FinCEN / IRS, and as are reasonably necessary, consistent with applicable law, to document the implementation and the operation of this Program.

L. Testing of the AML Policy

An independent audit function shall be responsible for reviewing the Program for compliance with laws and regulations, and internal policies and procedures. The Program shall be risk-assessed periodically by the AML Officer and members of the AML Team. Results will be shared with the Chief Compliance Officer, the Audit Committee of Sammons Financial Group, Inc, The Board of Directors and Senior Management.

Policy and Operating Standards

Name of Policy & Procedure	**Anti-Money Laundering Policy**
Primary Owner:	Mike Hagan

Summary of Key Rationale:

To update the Midland National Life Insurance Company and North American for Life and Health Anti-Money Laundering Policy to comply with federal laws and regulations, particularly the Bank Secrecy Act and the USA PATRIOT Act.

Will business units /departments have to prepare their own operating procedures [Y/N] Y

Comments:

The Financial Crimes Unit has reviewed the laws and regulations governing anti-money laundering that are applicable to Midland National Life Insurance Company and North American Company for Life and Health in the United States. As part of this review, the common requirements of federal laws, regulations and guidelines were identified and adapted for Midland National Life Insurance Company and North American Company for Life and Health's environment

Policy Administration

Approver(s):	• Mike Hagan, AML Officer • Jennifer Lewis, Legal Department • Cyndi Hall, Chief Compliance Officer
Owner(s):	Mike Hagan
Effective Date:	May 2, 2006
Last Revision Date:	July 1, 2019
Next Review Date:	December 2019 (dependent upon changes in regulatory and industry practice)
Version:	4.0

Version History

Version	Effective Dates	Reviewed / Written by:	Approved by:
1.0	5/02/2006 to 12/31/2008	Tracy Kirchoff	• Board of Directors
2.0	12/31/2008 to 11/01/2012	Jill Williams	• Tom Stavropoulos (Compliance) • Sarah Bouwman • Steve Horvat
3.2	11/1/2012 to 12/31/2017	Jill Williams	• Sarah Bouwman • Steve Horvat
4.0	7/1/2019	Mike Hagan	• Jennifer Lewis • Amy Teas (Legal) • Cyndi Hall (Compliance)