securian FINANCIAL™

Corporate Compliance

ANTI-MONEY LAUNDERING PROGRAM

Company Confidential

Last Reviewed Date: February 2025

TABLE OF CONTENTS

1. POLICY

It is the policy of Minnesota Life Insurance Company and Securian Life Insurance Company, (for the purposes of this Policy, collectively, "Securian Financial" or "Company") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with the Bank Secrecy Act ("BSA") and its implementing regulations.

Regulators have deemed money laundering to include any of the following types of activities:

- Engaging in financial transactions involving funds derived from criminal activities.
- Engaging in financial transactions in furtherance of criminal activity.
- Engaging in any activity designed to prevent detection of the fact that the funds were derived from criminal activity.
- Structuring, or participating in structuring, of transactions to evade money laundering reporting requirements.

1.01 DEFINITIONS

1.01.01 The Stages of Money Laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages: placement, layering, and integration. 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, traveler's checks, cashier'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 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.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or like methods used by other criminals to launder funds. Funding for terrorist attacks does not require large sums of money and the associated transactions may not be complex.

1.01.02 General Definitions

The following terms and their definitions are used throughout this Anti-Money Laundering Program:

Customer(s) shall include, but is not limited to client, accountholder, annuitant, insured, and policyowner.

Associate shall include all employees of Securian Financial, as well as employees designated as "contingent".

Account shall include but is not limited to insurance policy or annuity contract.

Transaction shall include but is not limited to deposits of money to pay premiums, deposits of contributions, withdrawals, or liquidations of funds from an insurance policy, annuity contract or account, or other monetary activities related to an account, policy, or contract.

We refers to Securian Financial, which is inclusive of Minnesota Life Insurance Company and Securian Life Insurance Company.

1.02 PURPOSE AND SCOPE

Securian Financials Anti-Money Laundering ("AML") Program is designed to ensure compliance with all applicable BSA regulations and other related SEC, Self-Regulatory Organization and Treasury regulations, and where applicable, relevant rules of the bank regulatory agencies. The program will be reviewed and updated on an annual basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations, in our business, or in other areas of the financial ecosystem.

The AML Program is also designed to ensure compliance with the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act of 2001) including Section 352 which requires the program to include the following elements:

- Development of internal policies and procedures.
- Appointment of an AML Compliance Officer.
- Ongoing training.
- Implementation of an Independent Audit function to test AML Program.

Securian Financials AML Program is based on an assessment of risk associated with Securian Financials customers, structure, size, products and services, sales force, distribution channels, cash processing practices, and other relevant factors. A risk assessment is conducted on an annual basis and the AML Program is updated if necessary.

1.02.01 Covered and Excluded Products

Products included in the Securian Financial AML Program (covered products) are:

- Permanent life insurance policies - other than group life insurance policies.
- Annuity contracts.
- Insurance products with cash value and investment features.

Products excluded from the Securian Financial AML Program are:

- Group insurance products.
- Term (including credit) life, property, casualty, health.
- Reinsurance contracts.

1.02.02 Out of Scope Entities

Other Securian subsidiaries or affiliates may be responsible for the design, implementation, and administration of AML programs for their entity's risks. Securian Financial will work with each of the subsidiaries providing guidance and partnering in AML related matters, when necessary.

1.03 THE IMPORTANCE OF AN AML PROGRAM FOR SECURIAN FINANCIAL

Federal law prohibits financial institutions from knowingly engaging in, or assisting with, money laundering activities. This concept of 'knowledge' is extremely broad, and a financial institution can be guilty of money laundering if it intentionally ignores certain suspicious activities. In addition to detecting and deterring money laundering activities, financial institutions also have a duty to report suspicious activities to the federal government.

Financial institutions and their associates are vulnerable to attempts by criminals to launder money. If such activities occur and Securian Financial determines that the Company or its associates knowingly participated in such activities, Securian Financial and/or the associate may be guilty of money laundering.

Although money laundering is usually associated with cash, it is not a required component in a transaction. Any financial transaction may be part of a process to obscure the origin of illegal funds. Day-to-day activities of Securian Financial associates can, theoretically, be part of a money laundering scheme including opening an account, processing checks, executing buy/sell orders, and processing transactions such as wire transfers and check withdrawals.

Therefore, Securian Financial associates need to understand what money laundering is, their role in identifying and combating it, and how to apply the policies and procedures of Securian Financials AML Program to their jobs. Failure to comply could result in significant criminal, civil, and disciplinary penalties including:

- Significant fines
- Loss of agency ratings
- Damaged reputation
- Employees of financial institutions can be fined individually and sentenced to up to 20 years of imprisonment for knowing or being willfully blind to the fact the transaction involved illegal funds

1.04 BOARD AND SENIOR MANAGEMENT APPROVAL OF THE AML PROGRAM

The AML Compliance Officer has approved the AML Compliance Program as reasonably designed to achieve and monitor Securian Financial's ongoing compliance with the requirements of the BSA and its implementing regulations.

The Chief Compliance Officer will be provided with a copy of the AML Program document every year or upon substantive revision. The AML Compliance Officer will consider program revisions, if any, as suggested by the Chief Compliance Officer

1.05 MONETARY INSTRUMENT POLICY (MIP)

It is the policy of Securian Financial to accept payments from clients in forms that minimize exposure to money laundering schemes and to document those payments that have been identified as presenting some level of increased risk. The Monetary Instrument Policy is reviewed on an annual basis.

Monetary Instruments that will be accepted:

- Personal checks
- Cashier's checks, official checks and bank drafts/checks with the name of the purchaser, account holder, or remitter preprinted on the check. The preprinted portion of the check should also provide confirmation of their affiliation as “purchaser,” “account holder” or “remitter.” For example, the subject line of the cashier's check should indicate “John Doe, purchaser" to provide reasonable assurances regarding the source of the funds.
- Certified checks
- Checks issued by an individual to Minnesota Life, Securian Life or affiliate on behalf of another when there is a business, familial or custodial account relationship between the remitter and contract owner.
- Credit card checks received via the lockbox.
- Checks issued by a business to Minnesota Life, Securian Life or affiliate on behalf of another for a transfer of assets.
- Checks issued by a bill-paying service to Minnesota Life, Securian Life or affiliate on behalf of an individual.
- Foreign checks and wires drawn on a foreign bank payable through a domestic correspondent bank.
- Wire transfers received through a domestic bank.
- ACH electronic transfers received through a domestic bank.

Monetary Instruments that will be rejected:

- Starter checks.
- Third-party checks (unless approved by the Cash Unit or for transfer of assets with FBO information on payee line).
- Foreign checks drawn on a foreign bank without a domestic correspondent bank.
- Credit card checks.
- Checks made payable to or from an agent or registered representative for someone else.
- Any check involving more than three parties.
- Cash will be rejected. Nominal amounts of cash accepted via U.S. mail will be tracked as an exception.
- Wire transfers received directly from a foreign bank.
- ACH electronic transfers received directly from a foreign bank.
- Money orders will be rejected. Any money orders received will be returned to the remitter.

2. DESIGNATION OF AML COMPLIANCE OFFICER AND DUTIES

The Corporate Compliance Officer and Chief Privacy Officer for Securian Financial is the company’s designated AML Compliance Officer. The AML Officer has working knowledge of the BSA and its implementing regulations and is qualified by experience, knowledge, and training; and has full responsibility and authority to enforce Securian Financials AML Program.

The AML Officer may delegate some of the duties of the AML Compliance Officer to the Special Investigations Unit (SIU) Manager, or the AML Risk Management Consultant (AML RMC). The SIU Manager and the AML RMC are responsible for overseeing the day-to-day AML Compliance Program.

The Securian Financial AML Compliance Officer, or their qualified designee(s), shall:

- Monitor Securian Financials compliance with AML obligations.

- Oversee the implementation of new AML requirements or changes to existing AML requirements.
- Ensure that appropriate Suspicious Activity Reports (SARs) are filed with FinCEN when appropriate.
- Ensure all required AML records are maintained.
- Provide periodic updates to the Chief Compliance Officer regarding the AML Program.
- Oversee the delivery of AML communications and training to associates.
- Interact with designated AML Compliance Officers of subsidiaries.

3. INFORMATION SHARING WITH GOVERNMENT AGENCIES AND OTHER FINANCIAL INSTITUTIONS

3.01 INFORMATION SHARING WITH GOVERNMENT AGENCIES – SEC 314(A)

Securian Financial will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (314(a) Request) by searching its records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure website. Unless otherwise stated in the 314(a) Request or specified by FinCEN, Securian Financial will search those documents outlined in FinCEN's FAQ.

For the match to be reportable, the policy/contract must be active at the time of reporting or have been active or open within the last 12 months. We will also report the match for any customers who have had a pending application within a 12-month period. If Securian Financial finds a match, it will be reported to FinCEN via FinCEN's web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (e.g., if FinCEN limits the search to a geographic location), Securian Financial will structure the search accordingly.

If Securian Financial searches its records and does not find a matching account or transaction, then it will not reply to the 314(a) Request. Securian Financial will maintain documentation that the required search has been performed. Such documentation will be maintained in the Sanctions Screening software system which will maintain a log of the number of accounts searched and whether a match was found.

Securian Financial will not disclose the fact that FinCEN has requested or obtained information, except to the extent necessary to comply with the information request. Securian Financial will review, maintain, and implement procedures to protect the security and confidentiality of requests from FinCEN like those procedures established to satisfy the requirements of the Gramm-Leach-Bliley Act regarding the protection of customers' nonpublic information.

Securian Financial will direct any questions regarding the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, Securian Financial will not be required to treat the information request as continuing in nature and will not be required to treat the periodic 314(a) Requests as a government-provided list of suspected terrorists for purposes of the customer identification and verification requirements.

3.02 VOLUNTARY INFORMATION SHARING WITH OTHER FINANCIAL INSTITUTIONS – SEC 314(B)

Securian Financial may share information regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering.

Prior to sharing information and annually thereafter, the Securian Financial Anti-Fraud and Financial Crimes Team will oversee the filing of the "Notification for Purposes of Section 314(b) of the USA Patriot Act and 31 CFR 1025.540" for Minnesota Life and Securian Life Insurance Company. Other applicable subsidiaries under Securian Financial Group, Inc. are responsible for filing the appropriate notification for their appointed 314(b) contacts.

Before Securian Financial shares information with another financial institution, Securian Financial will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. Securian Financial understands that this requirement applies even to financial institutions with which we are affiliated and that we will obtain the requisite notices from affiliates and follow all required procedures. Requests for information sharing from a financial institution that is not affiliated with Securian Financial should be referred to the appointed 314(b) contacts.

Securian Financial will employ appropriate procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from Securian Financials other books and records.

Securian Financial will also employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- Identifying and, where appropriate, reporting on money laundering or terrorist activities.
- Determining whether to establish or maintain an account, or to engage in a transaction.
- Assisting the financial institution in complying with performing such activities.

4. COMPARISON WITH GOVERNMENT LISTS

4.01 COMPARISON WITH THE OFFICE OF FOREIGN ASSETS CONTROL'S SDN LIST

Securian Financial will check to ensure that none of its customers, employees or vendors appear on OFAC's SDN list and are not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by the Office of Foreign Assets Control (OFAC). Generally, Securian Financial will scan the customer against the SDN list prior to opening an account and at least quarterly thereafter. Securian Financial will access the SDN list through a software program to ensure speed and accuracy. Because the SDN list and listings of economic sanctions and embargoes are updated frequently, Securian Financial will subscribe to receive available updates when they occur.

Securian Financial may rely on the performance of OFAC scans by a vendor or another financial institution before an account is opened when such reliance is reasonable under the circumstances.

If Securian Financial determines that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, Securian Financial will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. If needed, Securian Financial will also call the OFAC Hotline or use OFAC's e-hotline.

4.02 COMPARISON WITH GOVERNMENT-PROVIDED LISTS OF TERRORISTS

When Securian Financial receives notice that a federal government agency has issued a list of known or suspected terrorists, Securian Financial will, within a reasonable period after an account is opened (or earlier if required by another federal law, regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with federal functional regulators. Securian Financial will follow all federal directives issued in connection with such lists.

Securian Financial will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

More detailed information about Securian Financials OFAC Program can be found in the on Sync: https://sync.securian.com/content/dam/int/reg/ofac-compliance-program-F76945-1.pdf.

4.03 POLITICALLY EXPOSED PARTIES

A politically exposed person (PEP) is an individual that holds a position in a "prominent public function". A PEP (and by extension anyone closely related to a PEP) is more vulnerable to bribery or corruption by way of their position and any influence they may hold. Securian Financial collects additional financial suitability and beneficial ownership information for new contracts or additional coverage on existing customers, including if the account owner is a state or local government, an agency, or instrumentality of a state or local government. If yes, Securian Financial asks for them to disclose any political contributions.

5. KNOW YOUR CUSTOMER (KYC)

5.01 CUSTOMER DUE DILIGENCE

Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) are the foundation of a strong AML compliance program. Securian Financial performs CDD as part of the underwriting and suitability review processes for new individual life insurance policies and individual annuity contracts.

Securian Financial collects the following information:

- The purpose of the account.
- The source of funds and wealth.
- The beneficial owners of corporate owned accounts.
- The customer's occupation or type of business.

Based on this information, Securian Financial can better determine the customer's anticipated account activity including volume and type of transactions.

The CDD information is reviewed in connection with, and will provide a baseline for, evaluating customer transactions to determine whether the transactions are suspicious and need to be reported.

5.02 ENHANCED DUE DILIGENCE

In certain circumstances, Securian Financial may perform enhanced due diligence. Such circumstances include, but are not limited to:

- Clients owns a cash-intensive business
- Non-face-to-face client relationships
- Payment received from unknow or un-associated third parties
- Non-resident clients
- Identification of red flags
- Requests for contracts in excess of established limits
- Instances in which the customer does not match the target market for a product
- The business relationship is conducted in unusual circumstances (e.g., Significant unexplained geographical distance between the client and financial professional)
- Individual annuity contracts requiring heightened suitability reviews

5.03 IDENTITY VERIFICATION

Various legal and regulatory requirements require Securian Financial Group, Inc. and its affiliates to collect certain information to validate the identity of our customers. In response to this requirement Securian Financial has implemented a Customer Identification Program (CIP) to administer an effective anti-money laundering program.

Securian Financial is required to verify the identity of every customer opening an account. Any person, organization or entity agrees to have their identity verified by Securian Financial in accordance with the USA Patriot Act of 2001. This verification may include, but is not limited to, contact with financial institutions, consumer reporting agencies and government agencies.

Identity verification may be performed by the financial professional or Securian Financial's New Business team. The financial professional has the capacity to confirm the identification of the customer in person and attest to Securian Financial the authenticity of the documents through a few different forms. Securian Financial's New Business may use non-documentary means such as Instant ID or Accurint to verify the identity of the customer.

5.04 U.S. DEPARTMENT OF THE TREAUSRY 311 ACTIONS

Section 311 of the USA PATRIOT Act added 31 USC 5318A to the BSA, which authorizes the Secretary of the Treasury to require domestic financial institutions and domestic financial agencies to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts that are of primary money laundering concern. Section 311 provides the Secretary of the Treasury with a range of options that can be adapted to target specific money laundering or terrorist financing concerns, given that correspondent bank accounts have been used to facilitate illicit enterprises. Section 311 is implemented through various orders and regulations that are incorporated into 31 CFR 1010, Subpart F.

Securian Financial does not establish, maintain, administer, or manage correspondent accounts for foreign banks. A “correspondent account” is an account established by a financial institution for a foreign bank to receive deposits from; or to make payments or other disbursements on behalf of the foreign bank; or to handle other financial transactions related to the foreign bank.

Securian Financial is aware that a financial institution is prohibited from establishing, maintaining, administering, or managing a correspondent account for, or on behalf of, a foreign shell bank.

On an annual basis the AML Compliance Officer, or the AML RMC, will review the company’s products to ensure no changes have occurred that would allow such accounts to be opened or maintained. Upon finding or suspecting such accounts, Securian Financial associates must notify the AML Compliance Officer, who will terminate any verified correspondent accounts in the United States for a foreign shell bank. Securian Financial will also terminate any correspondent account that Securian Financial determines is not maintained by a foreign shell bank but is being used to provide services to such a shell bank. Securian Financial will exercise caution regarding liquidating positions in such accounts and take reasonable steps to ensure that no new positions are established in such accounts during the termination period. Securian Financial will terminate any correspondent account for which we have not obtained the information required in the regulations regarding shell banks within the time periods specified in those regulations.

Although Securian Financial does not maintain any accounts, including correspondent accounts, with any foreign jurisdiction or financial institution, if FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes or international transactions or types of accounts deeming them to be of primary money laundering concern, we understand that we must read FinCEN’s final rule and follow any prescriptions or prohibitions contained in that rule.

5.05 PRIVATE BANKING ACCOUNTS FOR NON-U.S. PERSONS

Securian Financial does not establish, maintain, administer, or manage private banking accounts. A “private banking” account is an account that requires a minimum aggregate deposit of $1 million, is established for one or more individuals and is assigned to or administered by an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

Securian Financial is aware that due diligence must be performed on all private banking accounts. In addition, enhanced due diligence must be conducted to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

On an annual basis the AML Compliance Officer, or the AML RMC, will review the company's products to ensure no changes have occurred that would allow such accounts to be opened or maintained. In the event such an account is discovered, Securian Financial will conduct due diligence on the account.

This due diligence will include at least:

- Ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information on those holders' lines of business and sources of wealth).
- Ascertaining the source of funds deposited into the account.
- Ascertaining whether any such holder may be a senior foreign political figure.
- Detecting and reporting, in accordance with applicable laws and regulations, any known or suspected money laundering, or use of the proceeds of foreign corruption.

If due diligence (or the required due diligence, if the account holder is senior foreign political figure) cannot be performed adequately, the AML Compliance Officer will determine whether to not open the account, suspend the transaction activity, file a SAR or close the account.

6. SUSPICIOUS ACTIVITY MONITORING

The detection and reporting of suspicious activity are keys to the deterrence of money laundering and terrorist activity.

Securian Financial monitors account activity for unusual size, volume, pattern, or type of transactions, considering risk factors and red flags that are appropriate to our business. Monitoring is conducted by associates in the business units manually reviewing transactions for suspicious customer behavior and transaction activity, including but not limited to, examples of money laundering red flag activity provided in Exhibit A. An associate who detects suspicious activity will bring it to the attention of their supervisor who will then submit a suspicious activity referral through our case management tool, i-Sight / Case IQ

The AML RMC will conduct reviews of potentially suspicious activity detected by the business units. The AML RMC will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR is filed.

The AML RMC is responsible for monitoring the business unit's review of any activity that is detected as possibly suspicious. The AML RMC will also determine whether additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

7. SUSPICIOUS ACTIVITY AND BSA REPORTING

7.01 SUSPICIOUS ACTIVITY REPORT FILING

Securian Financial will report to FinCEN any transaction that, alone or in the aggregate, involves at least $5,000 in funds or other assets, and Securian Financial knows, suspects, or has reason to suspect that it falls within one of following classes:

- The transaction involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity.
- The transaction is designed, whether through structuring or other means, to evade the requirements of the BSA.
- The transaction appears to serve no business purpose or apparent lawful purpose or is not the sort of transaction in which the customer would be expected to engage and for which Securian Financial knows of no reasonable explanation after examining the available facts.
- The transaction involves the use of Securian Financial to facilitate criminal activity.
- Confirmed cases of financial exploitations cases involving vulnerable adults

The above guidelines extend to patterns of transactions. Therefore, if Securian Financial determines that a series of transactions would not independently trigger suspicion, but when taken together, form a suspicious pattern of activity, Securian Financial will file a SAR. Also, if a transaction does not meet a specific dollar threshold that would trigger the filing of a SAR, but does raise an identifiable suspicion of criminal, terrorist, or corrupt activities, Securian Financial will appropriately review the transaction and determine if a SAR should be filed.

Securian Financial will also file a SAR and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes.

Securian Financial may file a SAR for any suspicious transaction that we believe is relevant to the possible violation of any law or regulation but that is not required to be reported under the SAR rule.

Securian Financial will report suspicious transactions by completing a SAR and will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of the initial detection, we may delay filing the SAR for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection. The phrase “initial detection” does not mean the moment a transaction is identified for review. The 30-day (or 60-day) period begins when an appropriate review is conducted, and a determination is made that the transaction under review is “suspicious” within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

Securian Financial will report any continuing suspicious activity on a previously filed SAR with a new filing at least every 90 days. Securian Financial will continue to assess whether it should continue to maintain the account or effect the transaction in question.

Securian Financial will retain copies of any SARs filed and the original or business record equivalent of any supporting documentation for at least seven years from the date of filing the SAR. We will identify and maintain supporting documentation and make such information available to FinCEN, the SEC or any other appropriate law enforcement agencies upon request.

Securian Financial will not notify any person involved in the transaction that the transaction has been reported, except as permitted by BSA regulations. In the event Securian Financial is subpoenaed or required to disclose a SAR or the information contained in the SAR, we will decline to produce the SAR and any information that would disclose that an SAR was prepared or filed, except where disclosures are requested by FinCEN, the SEC or another appropriate law enforcement or regulatory agency. Securian Financial will notify FinCEN of any such request and our response.

7.01.01 Exceptions to Filing a Suspicious Activity Report

Securian Financial is not required to file a SAR to report as the result of:

- A robbery or burglary that is reported by Securian Financial to appropriate law enforcement authorities.
- Lost, missing, counterfeit, or stolen securities with respect to which Securian Financial files a report pursuant to the reporting requirements of 17 CFR 240.17f-1.
- A violation of the federal securities laws or rules of a self-regulatory organization by Securian Financial, its officers, or associates, which is reported appropriately to the SEC or self-regulatory organization, except for a violation of Rule 17a-8 under the Securities Exchange Act of 1934, which must be reported on a SAR.

7.02 JOINT FILING OF SARS BY BROKER-DEALERS AND OTHER FINANCIAL INSTITUTIONS

Securian Financial will file a joint SAR if Securian Financial and another financial institution that is subject to the SAR regulations are involved in the same suspicious transaction. For example, Securian Financial and Securian Financial Services, Inc. (SFS) may file one SAR with respect to suspicious activity involving the sale of variable insurance products. If a joint SAR is filed, Securian Financial will maintain a copy of the SAR and supporting documentation in accordance with BSA recordkeeping requirements.

If Securian Financial determines it is appropriate to jointly file a SAR, we understand that we cannot disclose that we have filed a SAR to any financial institution except the financial institution that is filing jointly. If we determine it is not appropriate to file jointly, we understand that we cannot disclose that we have filed a SAR to any other financial institution or insurance company.

7.03 STATE REPORTING REQUIREMENTS

Certain states have enacted their own reporting requirements which may or may not be satisfied by reporting to the federal government. Consequently, whenever any type of transaction report under the BSA is filed with the federal government, Securian Financial will undertake efforts to analyze relevant state law to determine whether a duplicate or comparable form needs to be filed with a state authority.

7.04 SAFE HARBOR PROVISIONS

Federal law provides broad “safe harbor” protection from civil liability for the filing of SARs to report suspected or known criminal violations and suspicious activities, regardless of whether such reporting is mandatory or is done on a purely voluntary basis. The BSA provides that a financial institution and its directors, officers, associates, and agents who file a SAR “shall not be liable to any person” for such disclosure or for any failure to notify the person involved in the transaction or any other person of such disclosure.

7.05 FORM 8300

Securian Financials Monetary Instruments Policy prohibits the receipt of cash and currency as defined in the instructions for Form 8300 reporting (https://www.irs.gov/businesses/small-businesses-self-employed/form-8300-and-reporting-cash-payments-of-over-10000). If Securian Financial discovers such transactions have occurred, Securian Financial will file a Form 8300 with FinCEN for currency transactions that exceed $10,000. Securian Financial will treat multiple transactions involving currency as a single transaction for purposes of determining whether to file a Form 8300 if the transactions total more than $10,000 and are made by or on behalf of the same person during any one business day.

Although Securian Financial does not accept currency, cashier's checks are accepted only if the customer's name is printed on the check. Cashier's checks in amounts less than $10,000 are tracked by the Treasury Cash Unit. Securian Financial will file a Form 8300 or SAR if we know the payer is trying to avoid the reporting of such a transaction on Form 8300.

The Treasury Cash Unit monitors incoming monetary instruments, and the receipt of cash and cash-like instruments are recorded in the Cash Tracking database. The Treasury Cash Unit will notify the Anti-Fraud and Financial Crimes team upon receipt of cashier's checks that total more than $10,000 in a rolling calendar year for the same policy and/or client. The AML Officer, or the AML RMC, will then determine whether additional action is required, including whether a Form 8300 or Suspicious Activity Report should be filed.

7.06 CURRENCY AND MONETARY INSTRUMENT TRANSPORTATION REPORTS (CMIR)

Securian Financials Monetary Instruments Policy prohibits the receipt of currency. Securian Financial will file a Currency and Monetary Instrument Transportation Report (CMIR) with the Commissioner of Customs if we discover that we have received, caused, or attempted to receive from outside of the United States, currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time. We will also file a CMIR if we discover that we have physically transported, mailed or shipped or caused or attempted to physically transport, mail or ship by any means other than through the postal service or by common carrier, currency or other monetary instruments of more than $10,000 at one time.

7.07 REPORT OF FOREIGN BANK AND FINANCIAL ACCOUNTS (FBAR)

Securian Financial will file a Report of Foreign Bank and Financial Accounts for any financial accounts in a foreign country of more than $10,000 that we hold, or for which we have signature authority over. These accounts are tracked, and reports are filed by an individual in Securian's Corporate Tax department.

The form must be electronically filed using FinCEN's BSA E-filing System. For each calendar year, the form must be filed by June 30 of the following year.

7.08 WIRE TRANSFERS OF $3,000 OR MORE UNDER THE "JOINT AND TRAVEL RULE"

Securian Financial does not issue bank checks or drafts, cashier's checks, money orders or traveler's checks in the amount of $3,000 or more.

Under Treasury's Joint and Travel rule, when Securian Financial wire transfers funds, Securian Financial will create a paper trail by which enforcement officials can trace the transfer of such funds. At a minimum, Securian Financial will record in writing the following information:

- Name and address of the sender and recipient
- Amount of the transmittal
- Identity of recipient's financial institution
- Account number of the recipient
- Date of the transaction

8. AML RECORDKEEPING

8.01 RESPONSIBILITY FOR REQUIRED AML RECORDS AND SAR FILINGS

Securian Financials AML Compliance Officer is responsible for ensuring that the AML records are maintained properly, and that SARs are filed as required.

In addition, as part of our AML program, Securian will create and maintain SARs, Form 8300s, CMIRs, FBARs and relevant documentation on funds transmittals. We will maintain SAR and accompanying documentation for at least seven years. Minnesota Life and Securian Life will maintain other documents according to existing BSA and other recordkeeping requirements, including certain SEC rules that require six-year retention periods and Securian Financials Information Governance Program.

8.02 SAR MAINTENANCE AND CONFIDENTIALITY

Securian Financial will hold SARs and any supporting documentation confidential. We will not inform anyone outside of FinCEN, the SEC, or other appropriate law enforcement or regulatory agency about a SAR filing. We will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed. Securian Financial will notify FinCEN of any such subpoena requests that are received. We will segregate SAR filings and copies of supporting documentation from other books and records to avoid disclosing SAR filings. Securian Financials AML Compliance Officer, or the AML RMC, will oversee all subpoenas or other requests for SARs. We may share information with another financial institution about suspicious transactions to determine whether to file a joint SAR. In cases in which we file a joint SAR for a transaction that has been handled by Minnesota Life and Securian Life and another financial institution, both financial institutions will maintain a copy of the filed SAR.

It is our policy that all SAR filings will be reported to the Chief Compliance Officer on a regular basis. A review of any individual SAR filings will be provided with a clear reminder of the need to maintain the confidentiality of the SAR.

9. AML TRAINING

9.01 ASSOCIATE TRAINING

The Securian Financial AML Program training is developed and maintained by the AML RMC and meets the following requirements:

- Occurs at least annually.
- Is required for all associates with administrative responsibility for covered products.
- Is reviewed and updated as necessary, to reflect new developments in the regulation.
- Documentation evidencing completion of training is maintained in accordance with records retention requirements.
- Is included in the scope of the periodic (commensurate with the risks posed by Securian Financials covered products) AML audit conducted by the Internal Audit Department.

Associates whose job responsibilities require AML training may include, but are not limited to, associates who open accounts, handle client checks or wire transfers, or process client transactions, and associates who supervise such associates.

9.01.1 Training Program Content

Securian Financials AML Training Program includes, but is not limited to, information that provides an understanding of money laundering activities, prevention and detection methods, and regulatory requirements. Basic AML training content includes:

- How to identify red flags and signs of money laundering that may arise during the employee's duties.
- What to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis).
- The employees' role in the AML Compliance program and how to perform them.
- The disciplinary consequences including civil and criminal penalties for noncompliance with the BSA.

The development of AML training may be delegated to appropriate persons selected by the AML Compliance Officer. Specialized content will be identified and may be developed by management of the areas in need of such training.

9.01.2 Training Program Implementation

Training records will be maintained in accordance with the Securian Financial Records Retention Schedule.

Delivery of AML training may be through on-line industry courses, web-ex, educational pamphlets, videos, intranet systems, in-person lectures, explanatory memos, and other methods.

9.02 FINANCIAL PROFESSIONAL TRAINING

Securian Financial distributes covered products through a network of financial professionals. These financial professionals are required to complete anti-money laundering training on a biennial basis and provide proof of completion per Section 6.A of the Securian Financial Life Insurance and Annuity Sales Policies and Procedures guide:

> **A. Anti-money-laundering Policies**
>
> The Companies are committed to prohibiting and preventing money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Our anti-money-laundering programs provide information and guidance concerning the prevention of money laundering, which is an enforcement priority of the federal government, the U.S. Department of the Treasury, the Securities and Exchange Commission and the Office of the Comptroller of the Currency. In accordance with the USA Patriot Act, all producers appointed to sell the Companies' products must complete anti-money-laundering training on a biennial basis and provide proof of completion to the Companies. Please refer to the Companies' Anti-money-laundering Program available at **securian.com/policies**.

Securian Financial partners with a third-party vendor, LIMRA, to administer an "Insurance and Anti-Money Laundering Training" course. Financial professionals are provided with a link and login information to access the training and Securian Financial is automatically notified once training is completed. Training other than through LIMRA will be accepted, but proof of completion must be provided to Securian Financial.

If a financial professional is out of compliance with the training requirements a communication, by either email or physical mail, will go out to the financial professional advising them they have 30 days to take the training, or it may result in a suspension to submit business or possibly termination of their appointment with Securian Financial.

10. AML PROGRAM TESTING

10.01 INDEPENDENT TESTING

The audit of Securian Financials AML program will be performed on an annual basis commensurate with the risks posed by Securian Financials covered products, by the Internal Audit Department in coordination with the Anti-Fraud and Financial Crimes team and may include:

- Evaluating the overall integrity and effectiveness of Securian Financials AML Compliance Program.
- Evaluating Securian Financials procedures for BSA reporting and recordkeeping requirements.
- Evaluating internal monitoring program and, if necessary, perform additional testing of Securian Financials transactions with an emphasis on high-risk areas.
- Evaluating adequacy of training programs.
- Evaluating process for identifying suspicious activity.

- Evaluating process for reporting suspicious activity.
- Evaluating policy for reviewing accounts that generate multiple SAR filings.
- Evaluating Securian Financials response to previously identified deficiencies.

The scope of the audit will be determined by the Internal Audit Department. Audit findings, including recommendations to remedy any deficiencies, will be reported to the Securian Financial AML Compliance Officer. The Securian Financial AML Compliance Officer will be responsible for evaluating and implementing any recommendations and will have final approval authority over action dates and assignments established in response to Audit Improvement Agreements. The Securian Financial AML Compliance Officer will also determine additional distribution of the final audit report.

10.02 QUARTERLY TESTING

In alignment with the Minnesota Life Anti-Money Laundering Program, a quarterly report was developed to ensure compliance with Anti-Money Laundering regulations and ensure appropriate implementation of various policies and procedures. The quarterly report will be provided to the SIU Manager and the AML Compliance Officer for review upon completion.

The testing was developed to review various aspects of our Anti-Money Laundering program, including:

1. The adequacy of our CIP documentation prepared by associates in Individual Life and Individual Annuity.
2. The adequacy of review of monetary transactions processed by Individual Life, Individual Annuity and Treasury to ensure adherence with our Monetary Instruments Policy.
3. Verification of FinCEN 314(a) scanning and reporting.
4. Verification of OFAC scanning and reporting.
5. Verification of any Form 8300 filed.

11. CONFIDENTIAL REPORTING OF AML VIOLATIONS

11.01 CONFIDENTIAL AND ANONYMOUS REPORTING

Securian Financial associates will report any violations of Securian Financials AML Program to the AML Compliance Officer, unless the violations implicate the AML Compliance Officer, in which case the associate shall report to the Securian Financial Chief Compliance Officer. Such reports will be confidential.

If the associate would like to remain anonymous when reporting AML violations they can use the confidential Ethics Hotline at 1-877-215-1322 or securianethicsline.ethicspoint.com.

11.02 WHISTLEBLOWER PROTECTION

Securian associates may not retaliate against a whistleblower for reporting an activity, which that person believes to be an AML violation, with the intent or effect of adversely affecting the terms or conditions of employment (including, but not limited to, threats of physical harm, dismissal, transfer to an undesirable job assignment, demotion, suspension, or impact on salary or wages). Whistleblowers who believe that they have been retaliated against may file a complaint with Human Resources, the confidential Ethics Hotline at 1-877-215-1322 or securianethicsline.ethicspoint.com.

12. REVISION HISTORY

Major content revisions require approval by the accountability party assigned to the policy. Minor revisions (e.g., spelling, grammar, structure) completed do not require approval by the accountability party.

Change Description	Approved By	Approval Date	Version
Updated our retention timeframes from five to seven years to match our retention schedule on Sync.	Amanda Kelting	09/23/2022	
Minor changes to punctuation, clarification regarding the role of the AFFC leader's duties	Erich Axmacher	12/11/2022	
Integration of PwC recommendations and reformatting of some sections	Erich Axmacher	02/07/2024	February 2024
1. Removed Ochs, Inc. rom the AML Program document since they no longer sell covered products. 2. Removed language around board approval. 3. Removed language around reporting to the board. 4. Added review schedule for Monetary Instrument Policy. 5. Clarification around what is included in quarterly testing.	Erich Axmacher	02/25/2025	February 2025

6. Added link to the OFAC Compliance Program doc on Sync. 7. Clarification around CDD on annuity products. 8. Added in note about using i-Sight/Case IQ for referrals. 9. Clarification around SAR information provided to the Chief Compliance Officer. 10. Designees specified as SIU Manager or AML RMC.			

EXHIBIT A – MONEY LAUNDERING RED FLAGS

Certain red flags may signal possible money laundering or terrorist financing activities. The following list of money laundering and terrorist financing red flags may be noted at the point of sale or while processing a transaction. Their presence may indicate the need to notify the Securian Financial AML Compliance Officer to determine if the situation warrants further investigation and possible filing of a SAR.

i. New Business

- Use of starter checks
- Cashier's Checks missing client's name.
- Payments received from account without an identified relationship to the policy owner.
- The residential address is not consistent with the annual income and net worth noted on the application.
- Annual income/net worth does not support the coverage amount recorded on the application.
- Applicant is unemployed.
- Residence or employment address is a PO Box or mail facility.
- Out of state address and/or address significantly distant from agent.
- The producer consistently resists providing third-party verification of finances.
- Income, net worth, and/or liquid net worth listed on application are inconsistent with that obtained via telephone history interview, credit report, IRS transcripts/returns, third-party financials, etc.
- Occupation listed only as “owner” or “self-employed”, but no other specific information is supplied.
- Applicant’s business has no website or other web presence.
- Attempts to pay in cash or other prohibited cash equivalents.
- Agent requests withdrawal of application if verification of application information requested.
- Application lists no other insurance coverage or policies applied for, however, the phone history interview and/or MIB indicates other policy activity.
- The customer is from or has accounts in a country identified as a non-cooperative country or territory.
- The customer gives a false or stolen SSN.
- 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 unusual concern about Securian Financials compliance with government reporting requirements and Securian Financials AML policies (particularly concerning their identity, types of business and assets), or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspicious identification or business documents.
- The occupation stated by the customer is not commensurate with the level or type of potential activity for the account.
- Unexplained inconsistencies of data are noted during the process of identifying or verifying a customer.
- The purpose for opening an account for non-profit or charitable organization appears to have no economic purpose or link between the stated mission of the organization and other parties to the transaction.
- The customer requests that the account opening transaction be processed to avoid Securian Financials normal documentation requirements.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for funds and other assets.
- The customer is always in a rush.

ii. Financial Professional / Sales

- Lack of interest in policy features, coverages, etc. Interest expressed in surrender or cancellation process.
- The customer makes an unusual request, such as asking for help in converting cash into checks.
- The customer conducts its business under unusual circumstances, at irregular hours or in unusual locations.
- The customer offers gifts or gratuities greater than Securian Financials policies allow after being informed of Securian Financials policies.
- The customer (or someone connected with the account) is the subject of news reports or rumors indicating possible criminal regulatory, or civil fraud violations.
- The customer (or someone connected with the account) is the subject of inquiry or investigation by a regulatory or criminal prosecutorial agency.
- The customer's source of funds or other assets appear to be well beyond the resources of the person or entity.
- The information provided by the customer that identifies legitimate sources for funds is false, misleading, or substantially incorrect.
- The customer is always in a rush.
- Purchase of a product inconsistent with the customer's needs
- Purchase (or funding) of a product that appears to exceed a customer's known income or liquid net worth.
- Large payments made via multiple smaller payment amounts (multiple checks, money orders or cashier's checks from multiple banks, or a combination thereof)
- Little or no concern by a customer for the performance of a product that they purchased.
- Heightened concern about fees assessed for early termination of a product.
- Inquiries about paying in cash and/or money orders to avoid tax reporting.

iii. Transaction Processing – Money In/ Money Out

- The customer is always in a rush.
- Payments from third parties.
- Payments from multiple seemingly unrelated sources
- Premium overpayments that include or result in requests to send refunds to an address unrelated to previous policy activity.
- Initial premium returned as NSF or account closed.
- Money orders, wire transfers or cashier's checks frequently used to pay premiums.
- The same checking or savings account used to pay premiums for multiple unrelated insureds or multiple extended family members of the agent.
- The customer exhibits a lack of concern regarding risks, commission, or other transaction costs.
- The customer seeks to change or cancel a transaction after being informed that a report will be filed or that information will need to be verified.
- A customer who borrows the maximum amount soon after purchasing the product
- The customer engages in excessive journal entries between unrelated accounts with no apparent business purpose.
- The customer makes deposits or premium payments with multiple monetary instruments purchased from the same and/or different financial institutions.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- The customer account has unexplained or sudden extensive wire activity, where previously there had been little or no wire activity.

- The customer's transactions are unusual or inconsistent with the customer's normal trading practices.
- Unexplained or negotiation of third-party checks
- The source of funds is suspicious, such as transfers from a bank or other type of account that do not appear to have a legitimate relationship with the business.

iv. Business Operations (Processing)

- The customer gives a false or stolen SSN.
- Surrender or maximum loan requests shortly after policy issue without regard or concern for surrender fees. Includes request to send funds to a bank, business or address unrelated to previous policy activity.
- Legal entity is known to be associated with a terrorist organization or conducts business in a jurisdiction that has been designated by the U.S. as a primary money laundering concern or has been designated as non-cooperative by an international body.
- There is overlap between corporate officers or other identifiable similarities associated with addresses, references, and anticipated financial activities.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business or investment strategy.
- 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 is always in a rush.
- The customer maintains multiple accounts or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer makes a fund deposit followed by an immediate request that the money be withdrawn or transferred to a third party, or to another business without any apparent business reason.
- The customer makes investments that do not make economic sense, such as large sums sitting in a money market account.

v. Underwriting

- The residential address is not consistent with the annual income and net worth noted on the application.
- Annual income/net worth does not support the coverage amount recorded on the application.
- Applicant is unemployed.
- Residence or employment address is a PO Box or mail facility.
- Income, net worth, and/or liquid net worth listed on application are inconsistent with that obtained via telephone history interview, credit report, IRS transcripts/returns, third-party financials, etc.
- Occupation listed only as "owner" or "self-employed", but no other specific information is supplied.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating criminal, civil, or regulatory violations.
- The occupation stated by the customer is not commensurate with the level or type of potential activity for the account.