MassMutual Anti-Money Laundering (AML) Policy Summary

Date revised: 9/3/2026

Policy Status

This document is a summary of the Company's Anti-Money Laundering (AML) Policy and program. It contains the principal corporate-wide AML policy commitments of Massachusetts Mutual Life Insurance Company ("MassMutual") and its applicable subsidiaries and is part of the Company's broader AML compliance program.

Purpose

MassMutual and its subsidiaries (collectively, the "Company") are committed to preventing the use of its products, services, distribution channels, and operations for money laundering, terrorist financing, sanctions evasion, or other illicit financial activity. This AML Policy Summary contains the essential features of the Company's AML Policy and describes the corporate wide commitments, governance, and minimum standards that support the Company's risk-based AML program. The Company maintains its AML Policy and AML program to comply with applicable federal, state, and international AML laws and regulations, including the Bank Secrecy Act ("BSA"), the USA PATRIOT Act, FinCEN regulations, and, where applicable, FINRA Rule 3310 and Office of Foreign Assets Control ("OFAC") requirements.

Scope

The AML Policy applies to MassMutual and its subsidiaries to the extent applicable based on their business activities, regulatory status, and jurisdiction of operation. Each covered legal entity is responsible for implementing AML procedures and controls tailored to its specific risks, products, customers, distribution channels, and regulatory requirements while remaining aligned with the corporate-wide AML program.

Definition of Money Laundering

Money laundering is generally defined as the process by which individuals or entities attempt to conceal or disguise the nature, source, ownership, or control of funds derived from illegal activity to make such funds appear legitimate. Money laundering typically involves three stages: placement, layering, and integration. Terrorist financing may involve funds derived from legitimate or illegitimate sources and is intended to support terrorist activities.

Governance and Oversight

AML Program Oversight

The Company maintains AML governance and oversight designed to establish consistent standards across applicable subsidiaries. Such governance provides for appropriate oversight, escalation, reporting, and coordination across relevant business units, consistent with applicable laws and regulations.

AML Officer

The Company designates one or more qualified AML Officers, as applicable by legal entity or business, with sufficient authority, independence, and resources to administer AML programs and policies applicable to their respective legal entity or business. The AML Officer is responsible for:

- Developing, maintaining, and updating AML policies and related AML procedures.
- Overseeing the implementation of entity-specific AML programs.
- Monitoring compliance with applicable AML and sanctions laws and regulations.
- Escalating material AML issues and risks to senior management and appropriate governance committees.
- Serving as the primary point of contact with regulators and law enforcement on AML matters.

Core Program Elements

Each covered entity's AML program includes the following core elements, designed and implemented in a risk-based manner:

Risk Assessment

Periodic AML risk assessments conducted to identify and evaluate money laundering and terrorist financing risks associated with products, services, customers, distribution channels, transactions, and geographic exposure.

Customer Identification and Due Diligence

Risk-based customer identification, verification, and due diligence measures, including:

- Customer Identification Program ("CIP") requirements, where applicable.
- Reasonable measures to identify and verify beneficial owners of legal entity customers, as required by law.
- Understanding the nature and purpose of the customer relationship.
- Enhanced due diligence for higher-risk customers, including foreign politically exposed persons ("PEPs"), as applicable.

Monitoring and Detection

Processes and controls designed to identify potentially suspicious activity, including unusual transactions or behavior that may indicate money laundering, terrorist financing, or other illicit activity.

Suspicious Activity Reporting

When required by law, suspicious activity escalation to the appropriate AML Officer for review and, if warranted, timely reporting to the appropriate governmental authority (e.g., Suspicious Activity

Reports ("SARs"). SARs and related information are maintained as confidential in accordance with applicable law.

Sanctions Compliance

The AML Program incorporates sanctions compliance requirements, including screening against OFAC lists and compliance with applicable economic and trade sanctions programs.

Training

Risk-based AML and OFAC training is provided to employees, agents, and other covered persons in accordance with their roles, regulatory requirements, and responsibilities under this AML Policy and related procedures. Training is designed to address:

- AML obligations and regulatory expectations.
- Identification of red flags and suspicious activity.
- Escalation and reporting requirements.
- Potential civil and criminal penalties for non-compliance.

Independent Testing

The AML program is subject to independent testing on a periodic, risk-based basis to assess the effectiveness of program design and implementation. For those affiliates subject to FINRA Rule 3310, such testing is conducted at least annually and is reasonably designed to assess compliance with FINRA Rule 3310 and related regulatory requirements. Identified deficiencies are tracked and remediated in accordance with established governance and oversight processes.

Policy Review, Approval, and Maintenance

The AML Policy is reviewed periodically and updated as necessary to reflect changes in laws, regulations, regulatory guidance, and the Company's risk profile. Material changes are subject to appropriate governance review and approval, and the policy is administered as a formal Company commitment through documented ownership, version control, effective dating, and training or communication as appropriate.