

UNUM

USA Patriot Act
Compliance Program

Anti-Money
Laundering
Policy

Table of Contents

- 1.0 [INTRODUCTION](#)
 - 1.1 Ownership
 - 1.2 Anti-Money Laundering Compliance Officer
 - 1.3 Purpose of Policy

- 2.0 [MONEY LAUNDERING](#)
 - 2.1 Money Laundering Process
 - 2.2 Individual Employee Duties

- 3.0 [INSURING COMPANIES](#)
 - 3.1 Product and Service Risk Assessment
 - 3.2 Know Your Customer Guidelines
 - 3.3 Red Flags

- 4.0 [OTHER BUSINESS RELATIONSHIPS](#)

- 5.0 [REPORTING](#)
 - 5.1 Suspicious Activity Report
 - 5.2 Monitoring for Suspicious Activity
 - 5.3 Confidentiality

- 6.0 [TRAINING](#)

- 7.0 [RECORDKEEPING REQUIREMENTS](#)

- 8.0 [SELF-ASSESSMENT](#)

[Exhibit A](#) Risk Assessment Guidelines and Results of Product and Portfolio Service Review

[Exhibit B](#) Know Your Customer Guidelines

[Exhibit C](#) Suspicious Transaction Guidelines - Red Flags

[Exhibit D](#) Suspicious Activity Report (SAR) Worksheet

1.0 INTRODUCTION

The attempted use of financial institutions to launder money is a significant problem that has resulted in the passage of stricter laws and increased penalties for money laundering including the USA Patriot Act. This Anti-Money Laundering Policy ("Policy") is designed to establish principles and standards to protect against attempts at laundering money through Unum Group and its United States subsidiaries ("Unum").

This Policy is to be used to create an understanding among employees concerning the risks of laundering money and the penalties for failing to comply with the procedures outlined herein. This Policy establishes the minimum standards to which Unum must adhere. In any case where the requirements of applicable anti-money laundering laws establish higher standards, Unum will adhere to those laws. Implementation of the Unum Anti-Money Laundering Program is predicated upon a careful analysis of the final rules for insurance companies issued by the U.S. Treasury Department, assessment of the vulnerabilities of our business to money laundering, and adoption of controls appropriate to that risk.

1.1 Ownership

This Policy is applicable to Unum and is enforced by the Unum [Anti-Money Laundering Compliance Officer](#). Changes to the Policy may be made only with the approval of the Anti-Money Laundering Compliance Officer. Exceptions to the policies and procedures contained herein are permitted only upon the express consent of the Anti-Money Laundering Compliance Officer.

1.2 Anti-Money Laundering Compliance Officer

Unum shall be served by an [Anti-Money Laundering Compliance Officer](#) or other designated business/supervisory personnel responsible for coordinating and monitoring day-to-day compliance with this policy and applicable Anti-Money Laundering laws and regulations. The Anti-Money Laundering Compliance Officer or other designated business/supervisory personnel may serve other functions and may serve multiple business units. Unless specifically designated otherwise, the Vice President of Business Practices and Ethics of Unum shall be the Anti-Money Laundering Compliance Officer.

1.3 Purpose of Policy

This policy contains procedures to ensure that Unum complies with applicable anti-money laundering laws and regulations and protects against money laundering attempts by:

- introducing Unum employees to the stages of the Money Laundering process and to their individual duties,
- establishing a review process which will be used to identify opportunities that might be used to launder money,
- defining Guidelines that will promote knowing who our customers are,
- providing instructions regarding taking appropriate action once a suspicious activity or a money laundering activity is detected or suspected, and
- describing anti-money laundering training requirements.

1.4 Scope

For purposes of this policy, the term "covered product" is defined to mean:

- 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

With respect to First Unum Life Insurance Company, Unum Life Insurance Company of America, Provident Life and Accident Insurance Company, Provident Life and Casualty Insurance Company, and Paul Revere Life Insurance Company, this policy applies to:

- VWB Universal Life – VIUL, Fortune, PS 1000
- VWB Interest Sensitive Whole Life – ISWL, PS Plus
- Individual Annuities

With respect to Colonial Life and Accident Insurance Company, this policy applies to:

- All universal life policies, such as Universal Life – Policy UL 97
- All whole life policies, such as Lifebridge 96 (Whole Life) – Policy LBCDGP (96)

2.0 MONEY LAUNDERING

Money laundering is not merely an attempt to disguise money derived from the sale of drugs. Rather, money laundering is the involvement of any transaction or series of transactions seeking to conceal or disguise the nature or source of proceeds derived from illegal activities, including drug trafficking, terrorism, organized crime, fraud, and other crimes.

2.1 The Money Laundering Process

Generally, the money laundering process involves three stages:

1. Placement – Physically disposing of cash derived from illegal activity. One way to accomplish this is by placing criminal proceeds into insurance products or with other financial institutions or non-traditional financial institutions such as currency exchanges, casinos, or check-cashing services.
2. Layering – Separating the proceeds of criminal activity from their source through the use of layers of financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity. Examples of layering include irregular payment patterns to an insurance contract, which is then surrendered and a disbursement of funds is provided.
3. Integration – Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

The degree of sophistication and complexity in a money laundering scheme is infinite, limited only by the creative imagination and expertise of the perpetrator. It is possible for a person with criminal intent to make use of a financial institution, such as an insurance company, at any point in the money laundering process.

2.2 Individual Employee Duties

Unum expects that its employees will comply with applicable money laundering laws. Unum also expects that its employees will conduct themselves in accordance with the highest ethical standards.

Unum employees are prohibited from providing advice or other assistance to individuals who attempt either to violate or avoid anti-money laundering laws or this Policy. Such assistance may include, but is not limited to, approving suspicious applications or new group accounts, or the failure to

thoroughly analyze the source of client funds, or failing to meet obligations as outlined in this Policy.

Unum employees whose suspicions are aroused by suspicious activities (which will be more fully described later in this Policy), but who fail or neglect to make further inquiries, may be considered to have knowledge of such activity. Unum employees who suspect money laundering activities must refer the matter to the [Anti-Money Laundering Compliance Officer](#).

Failure to adhere to this Policy may subject Unum employees to disciplinary action up to and including termination of employment. Violations of anti-money laundering laws may also subject Unum employees and the Company to fines, forfeiture of assets, and other serious punishment, including imprisonment.

2.3 Producer Duties

Unum expects that producers who are engaged in the marketing and sale of its products will play an important role in monitoring for money laundering risks. Unum expects its producers to review this Policy and be familiar with their obligations under it. For purposes of administering the Policy, Unum producers shall have the same obligations as those outlined for Unum employees, with "producer", "producer agreement", "producer relationship" and similar terms substituted for "employee", "employment", "employment relationship" or similar references.

3.0 INSURING COMPANIES

We have developed this Policy with the understanding that different money laundering risks arise depending on the type of insurance product sold, services provided and the distribution channel in which it is marketed. Accordingly, we have conducted a review of each of our products and services to determine if there is a risk that they may be used to launder money. We will also conduct a similar review when a new product, an enhancement to an existing product, a new service or an enhancement to an existing service is introduced. [Exhibit A](#) will be used to facilitate these activities.

Product and Service Risk Assessment

In developing this Policy, Unum established procedures for assessing the money laundering risks it currently faces, taking into account the following factors among others:

- The features in the products and services that are provided by Unum and what are their expected use by the customer;
- Whether the product has a means for distribution of funds; i.e. loans, cash values, large amount for return of premium, refunds from ASO business, etc.;
- The different categories of customers; i.e. who are the buyers of the product or service and how is it marketed; and
- What are the solicitation procedures; i.e. how are enrollments facilitated and what underwriting procedures are followed?

Each change to Unum's product portfolio and service will need to be reviewed pursuant to this Policy, and all products and services that hold a potential risk for facilitating money laundering must be brought to the attention of the [Anti-Money Laundering Compliance Officer](#).

In conjunction with the product portfolio and service risk assessment, a procedure for monitoring possible customer money laundering activities needs to be followed. An important step in monitoring money laundering is to know your customer.

Know Your Customer Guidelines: Identification and Source of Funds

This Policy provides a Guideline that defines the key components that need to be understood when establishing the identity of a customer. They are designed to:

- Determine and document the true identity of customers, including basic background information;
- Obtain and document any additional customer information, commensurate with the assessment of the money laundering risks posed by the customer's expected use of products and services; and
- Protect Unum from the risks associated with doing business with individuals whose identities cannot be determined.

Customer Identification

With regard to the identity of corporations, trusts, partnerships and other legal entities, Unum shall review documentation confirming the establishment or good standing of such entity. In some circumstances, Unum will require confirmation of the identities of shareholders, principals, trustees, partners or officers of such entities.

With regard to the identity of individual customers, whether the product or service is provided on a truly individual basis or through a multi-life arrangement, Unum shall review documentation confirming the establishment or good standing of such customer. This information is usually acquired during the underwriting process.

In the event that any person or entity represents themselves as having authority to act on behalf of the customer, then documentation, reference to local law or other reliable means shall be used to establish the identity and authority of such person or entity. Unum shall require proof that a person or entity has been authorized to act on behalf of a customer, including but not limited to, verifying power of attorney or other applicable documentation.

Unum shall gather information during the application process sufficient to support the "Know Your Customer Guidelines" (See [Exhibit B](#)). Such information will be provided on contract applications, new account forms, or other forms executed by the customer in the process of applying for Unum products. If the identity of the customer cannot be confirmed or does not provide appropriate protection for Unum, we should not enter into a business relationship with that customer.

Source of Funds

Except as detailed below, deposits and premium payments will be accepted only in the form of the personal check or wire transfer from the contract owner, policy owner, account owner or Third Party Administrator.

- We will not accept cash as payment, except under limited circumstances pre-approved by the Anti-Money Laundering Compliance Officer.
- In the case of wire orders, we should verify the source of funds prior to accepting any such wire order.
- Unum will not accept third party checks.
- No special name accounts (i.e., an account using a pseudonym or number rather than the actual name of the customer) will be permitted unless a legitimate business reason exists.
- Unum will not accept money orders or travelers checks, except under limited circumstances pre-approved by the Anti-Money Laundering Compliance Officer. The preferred method of payment is the purchaser's personal check; however, a bank cashier's or treasurer's check is an acceptable alternative.

Exceptions can be made if the annual amount is under \$500 and the customer's identification is confirmed separate from the time the coverage was issued. The [Anti-Money Laundering Compliance Officer](#) must approve any other exception prior to its submission.

Red Flags

In connection with sales of potentially risky products (i.e. those at risk for money laundering) or in the event that a "red flag" is triggered, additional due diligence is required. A list of possible "red flags" is provided in [Exhibit C](#). Unum will take steps to reasonably ensure that the product(s) applied for are suitable, given the nature and extent of the customer's expected use of its products and services. If, however, a situation arises that triggers a "red flag," the [Anti-Money Laundering Compliance Officer](#) must be notified.

4.0 OTHER BUSINESS RELATIONSHIPS

As Unum enters into business relationships with others, the purchasing or selling of assets, real estate, or other investments or the development of other partnerships, we must assess whether the venture has a risk for supporting the laundering of money. If it is determined that a risk is present, then we should not enter into business with the other party and the [Anti-Money Laundering Compliance Officer](#) should be contacted to make him aware of the situation. If we do not become aware of the risk until after we have entered into the relationship, then as soon as we are aware that a risk exists or that a suspicious activity has occurred the Anti-Money Laundering Compliance Officer should be contacted.

5.0 REPORTING

Once the [Anti-Money Laundering Compliance Officer](#) has been notified that there is a risk that we have been involved with a money laundering scheme or that we are suspicious that such an activity might occur, the process of reporting the activity will begin.

5.1 Suspicious Activity Report

U.S. regulations require Unum to send a Suspicious Activity Report, "SAR," to the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") when Unum knows, suspects, or has reason to suspect that any transaction conducted or attempted by, at, or through Unum:

- Which involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under federal law;
- Is designed to evade U.S. anti-money laundering regulations; or
- Has no business or apparent lawful purpose or is not the type of transaction in which the particular customer would normally be expected to engage, and Unum knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

In the event that a Unum business unit seeks to terminate a relationship because of suspicious activity, Unum shall observe the following procedures.

1. Promptly refer the matter to the [Anti-Money Laundering Compliance Officer](#), who will work with Unum's Special Investigative Unit, SIU, to notify the appropriate legal authorities.
2. Complete a Suspicious Activity Report Worksheet (see [Exhibit D](#)). The SAR Worksheet and the matter will be reviewed, and a SAR will be sent to the Department of Treasury's Financial Crimes Enforcement Network ("FinCEN").
3. Communicate the decision to terminate the relationship and the scheduled date for notifying the party(ies) of that decision.

5.2 Monitoring for Suspicious Activity

Unum will monitor its customer/partner relationships to detect any suspicious activities. Potentially suspicious activities include many ordinary transactions, which may be legitimate, but should be examined. Examples may include surrendering an individual life insurance policy, which has a cash surrender value in spite of penalties, or attempting to take large loans against contract values in a manner inconsistent with stated features and services of the product. Another example might be when a group case is sold on an Administrative Service Only basis and the plan is surrendered with a return of the claim reserves.

In the event that any suspicious activity is detected, employees will work with their managers and the Anti-Money Laundering Compliance Officer to complete a Suspicious Activity Report Worksheet (see [Exhibit D](#)). The SAR Worksheet and the matter will be reviewed. In addition, the Anti-Money Laundering Compliance Officer will work closely with the SIU to investigate suspicious or questionable activities and will forward, if necessary, a SAR to government authorities in accordance with applicable law.

5.3 Confidentiality

In the event Unum files a SAR, or otherwise reports suspected or known criminal violations or suspicious activities to law enforcement authorities, Unum employees must keep such reporting confidential.

No person other than the head of the SIU is authorized to contact any law enforcement official with respect to suspicious activities. The SIU shall make all referrals to law enforcement.

6.0 TRAINING

The Special Investigative Unit, SIU, will provide anti-money laundering training as needed on a periodic basis. Such training may take the form of written materials. These materials may at times be distributed electronically.

The training shall review applicable anti-money laundering laws and recent trends in money laundering activity to combat money laundering, including how to recognize and report suspicious transactions.

In conjunction with the Unum Anti-Money Laundering Compliance Officer, the head of the SIU will determine the frequency of training and which personnel must be trained based on their roles and job functions in relation to covered products.

7.0 RECORDKEEPING REQUIREMENTS

Unum shall have policies and procedures to comply with applicable record keeping and reporting requirements established by law.

Unum shall maintain the following documents for at least five years unless local law or the particular Unum business unit's document retention policy specifies a longer period:

- All Product Portfolio and Service Review documents submitted to the Anti-Money Laundering Compliance Officer;
- All Suspicious Activity Report (SAR) worksheets submitted to the Anti-Money Laundering Compliance Officer;
- Reports made to government authorities concerning suspicious activities relating to possible money laundering or other criminal conduct together with supporting documentation;
- Records of anti-money laundering training materials, including the agenda, locations, dates, and documents used during the training sessions; and
- Any other documents required to be retained under applicable anti-money laundering laws.

8.0 SELF-ASSESSMENT

Unum will conduct self-assessments of its anti-money laundering policies and procedures on a periodic basis to provide reasonable assurance that this policy and its procedures are effective. These self-assessments will be performed by an independent person(s) who is not involved in the administration of the Anti-Money Laundering program. They will not be conducted by the Anti-Money Laundering Compliance Officer or any member of Unum's Anti-Money Laundering office.

Exhibit A

Risk Assessment Guidelines and Results of Product Portfolio and Service Review

Each product and service associated with Unum's portfolio will need to be reviewed in conjunction with the Guidelines provided below. The review will be conducted with the Anti-Money Laundering Compliance Officer and staff from various functional areas.

All new products and/or services that are added to Unum's portfolio will have to be run through the Risk Assessment process.

Risk Assessment Guidelines

The following activities should be undertaken as a means of assessing the risk for exposure to money laundering:

- determine the expected use of each product feature and service that are provided by Unum,
- identify whether the product or service has a means for distribution of funds; i.e., loans, cash values, large amount for return of premium, refunds from ASO business, etc.,
- establish different categories of customers; i.e., who are the buyers of the product or service and how is it marketed, and
- evaluate the solicitation procedures; i.e., how are enrollments facilitated and what underwriting procedures are followed.

After analyzing the data collected, each product and service will then be assigned a "Risk Factor" of high, medium, low or no risk.



Exhibit A Product
and Service Review

Exhibit B

Know Your Customer Guidelines

For any "covered product, Unum shall gather and maintain information during the application process, which accurately identifies the customer. Such information may be contained in applications or other forms executed by the customer in the process of applying for Unum products. If the identity of the customer cannot be determined with sufficient certainty, we should not enter into a business relationship with that customer.

For any covered product, the company must have sufficient information on all policyholders to answer the following:

1. Who is the customer and what information do we have to accurately identify them, e.g. customer's name, customer's address, customer's phone number, group or individual customer ID , name of product or service, account/policy number, industry/occupation, social security/tax ID or other unique identifier, date of birth (if individual customer)...

If we do not have appropriate information to obtain the customer's identification, then we should not enter into a business relationship with that customer.

2. Are the product or service features appropriate for the customer?
If no, then we should not enter into a business relationship with that customer.
3. Are funds paid out of proportion to the expected premium cost or amount?
If yes, then we should not enter into a business relationship with that customer.
4. Do you anticipate that there will be large distribution of funds from the relationship?
If yes, then we should understand why before entering into a business relationship with that customer.
5. Is the insurance issued proportional to the risk being insured?
If no, then we should not enter into a business relationship with that customer.

Exhibit C

Suspicious Transaction Guidelines

"Red Flags"

If any of the following scenarios occur, immediately contact the Anti-Money Laundering Compliance Officer.

1. The customer seeks to make purchases with large amounts of cash, cash equivalent or checks drawn on different accounts.
2. The customer refuses or is reluctant to complete an application or to otherwise provide all the required information, or the information provided is false, inconsistent or suspicious in nature.
3. The customer attempts to purchase an insurance policy in an amount that is far beyond his, her or its apparent means that has no obvious purpose, or where the source or nature of the funds to be used is suspicious.
4. The customer wishes to buy an insurance product, but is less concerned with the cost, long-term performance, or economic terms than in early surrender or cancellation.
5. The customer seeks to cancel a contract without regard to penalties.
6. The customer demands policy loan or surrender value quickly after policy issuance.
7. There is no apparent relationship between the policyholder/owner and the insured or beneficiary.
8. The source of the customer's funds is unclear or inappropriate, or does not correspond with the customer's known business activities and financial situation.
9. Any activity involving suspected fraudulent sales activities on the part of an agent and/or broker.
10. Failure to comply with application submission or underwriting procedures and guidelines.

Exhibit D

Suspicious Activity Report (SAR) Worksheet

The questions contained on the Suspicious Activity Report Worksheet will facilitate the process of determining whether a suspicious activity report, or another report, is required to be filed under the Anti-Money Laundering Policy. If you suspect that money is being laundered through one of Unum's products or services or through one of our business relationships, then complete the form to the best of your ability and submit it to the [Anti-Money Laundering Compliance Officer](#).

Please remember to keep this process confidential. Release of this form or the information contained on it to anyone outside of the Unum Group is strictly prohibited.



Exhibit D SAR
Worksheet