

**Domestic Life Compliance  
Anti-Money Laundering  
(AML)  
Business Unit  
Procedure Manual**

---

## **Table of Contents**

<b>Mission Statement .....</b>	<b>5</b>
<b>Objective .....</b>	<b>5</b>
<b>Introduction .....</b>	<b>5</b>
Covered Companies.....	6
Non-Covered Companies.....	6
Covered Products.....	7
Excluded Products .....	7
Systems.....	8
<b>General Information .....</b>	<b>9</b>
RED FLAGS / SUSPICIOUS ACTIVITY INDICATORS.....	9
Producer .....	9
New Business / Underwriting .....	10
Policyowner Services.....	11
Premium Processing.....	11
Tax Haven Countries.....	12
OFAC Blocked Countries .....	12
<b>New Business and Underwriting .....</b>	<b>13</b>
IPO (Excluding Annuity) New Business Processing.....	13
CWA Initial Premium Payment Review.....	13
IPO Initial Application Review .....	15
CWA Refund Check.....	16
Houston Annuity New Business Processing.....	20
CWA Initial Premium Payment Review.....	20
CWA and 1035/ Trustee Transfer Refund Check under Free look/NTO .....	21
Wilmington Annuity New Business Processing .....	25
CWA Initial Premium Payment Review.....	25
Refund of Premium within Free Look Period .....	25
Wilmington Annuity Initial Application Review .....	26
EBS New Business Processing.....	31
Refund Check .....	31
EBS Initial Application Review .....	31
AGLA New Business Processing .....	36
Underwriter Initial Application Review.....	36
New Business Refund Check for Declined or Retired Applications .....	37
<b>Policyowner Services (POS) .....</b>	<b>42</b>
IPO (excluding Annuity) POS (including EBS) .....	42
Title Changes.....	42
Owner & Beneficiary Change .....	42
Address Change .....	42
Disbursements.....	43
Not Taken Offer (NTO).....	43
Surrender, Partial, & PDF/Prepay Withdrawal .....	43
Loan .....	43
Premium Payments.....	44
Premium Refund .....	44
AML Liaison .....	44

Houston Annuity Policyowner Services .....	54
Disbursements .....	54
Not Taken Offer (NTO).....	54
Premium Refund, Premium Paid in Excess of Contract.....	54
Surrenders, Partial Surrenders, & Systematic Withdrawal.....	54
Title Changes.....	55
Address/Owner & Beneficiary Change.....	55
Periodic Payments – Change of Payee.....	55
Annuity Compliance.....	55
Wilmington Annuity Policyowner Services.....	61
Disbursements .....	61
Refund of Premium within Free Look Period.....	61
Lockbox Exception Payments & Non-Lockbox Premium Procedures.....	61
Title Changes.....	61
Address Change .....	61
Owner & Beneficiary Changes .....	61
AML Liaison .....	62
AGLA Policyowner Services.....	69
Title Change .....	69
<i>Owner &amp; Beneficiary Change</i> .....	69
<i>Address Change</i> .....	69
Disbursements .....	69
<i>Not Taken Offer (NTO)</i> .....	69
<i>Surrender, Partial, &amp; Prepay Withdrawal</i> .....	70
<i>Loan</i> .....	70
<i>Premium Refund</i> .....	71
AML Liaison .....	71
AGLA Cash Payment Procedures .....	72
AGLA Monthly Compliance Procedures .....	73
<b>Treasury.....</b>	<b>83</b>
High Dollar Disbursement Review.....	83
<b>Licensing &amp; Commissions .....</b>	<b>85</b>
Notification of training requirement.....	85
Existing Agent.....	85
New Agent Appointment .....	85
Roll-Out Training program.....	85
LIMRA web-based AML program .....	85
AML training other than LIMRA.....	85
Follow-up for agent non-compliance .....	85
Pending Application Process .....	85
<b>Training.....</b>	<b>86</b>
Initial Training .....	86
Ongoing AML Training .....	86
<b>Global Watch List.....</b>	<b>87</b>
OFAC Team Procedures.....	87
Daily Check, Payryte & New Business runs & Weekly In force runs .....	87

<b>AML Compliance Committee .....</b>	<b>88</b>
<b>Reporting Suspicious Activity .....</b>	<b>89</b>
<b>APPENDIX A .....</b>	<b>90</b>
Business Policy 0315 .....	90
<b>APPENDIX B - SAR Form .....</b>	<b>99</b>

---

## Mission Statement

American General Domestic Life Operations will protect the interests of the organization and its shareholders by fostering an Anti-Money Laundering environment.

## Objective

To establish policies and procedures that provide Domestic Life employees and its agents the necessary tools to proactively prevent fraudulent money laundering activities transacted through the insurance industry.

To provide training that allows Domestic Life employees to recognize and act upon suspicious financial transaction-related activity.

## Introduction

Money Laundering is the process by which criminals conceal the nature or source of their illegal funds and disguise them to make them appear legitimate.

The Financial Crimes Enforcement Network (FinCEN) issued regulations requiring insurance companies to develop and implement an Anti-Money Laundering program and to define the companies and insurance products that are subject to the requirement. The Anti-Money Laundering Rules for Insurance Companies has the following 4 core components:

- Develop and implement policies, procedures, and internal controls
  - Business Policy – 0315 Anti-Money Laundering Policy (Appendix A)
  - Procedures – Anti-Money Laundering (AML) Procedure Manual
- Designate a Compliance Officer responsible for developing, implementing, & monitoring the AML program
  - American General AML Compliance Officer
- Provide ongoing training for “appropriate persons”
  - AML Training Course provided online as “web-based” training for:
    - Independent Producer
    - Captive Agent
    - Office Employee
- Provide for independent testing to monitor and maintain an adequate program
  - Internal Audit

**Another important aspect of a strong AML program requires that we “Know Our Customer.” Gathering, storing and maintaining key pieces of information about our clients is critical. While the systems may not ‘require’ certain fields be completed to submit, issue or make changes to a policy record, the input of the client’s full name, address, date of birth, citizenship and social security number are imperative for compliance to the AML regulation.**

### **SPECIAL DOCUMENTATION NOTE:**

***Throughout the individual sections of this manual, it is understood that all references to “the Company” refers to one or more of the American General Life Companies.***

---

## ***Covered Companies***

Unless otherwise stated elsewhere, the American General Domestic Life Companies covered under the procedures outlined in this manual are as follows:

AIG Life Insurance Company  
AIG Life of Bermuda, Ltd  
American General Life Insurance Company  
American General Life and Accident Insurance Company  
American International Life Assurance Company of New York  
Delaware American Life Insurance Company  
Pacific Union Assurance Company  
The United States Life Insurance Company in the City of New York

## ***Non-Covered Companies***

The following Domestic Life Companies have been reviewed and excluded based on various reasons such as type of products, location of market, &/or sufficient procedures in place.

AIG Worldwide Life Insurance Company of Bermuda, Ltd.  
AGC Life Insurance Company  
American General Assurance Company  
American General Equity Services Corporation  
American General Indemnity Company

---

## ***Covered Products***

The following products are covered by the regulation or based on the risk assessment:

Individual Universal Life  
Individual Variable Universal Life  
Individual Fixed Annuity  
Individual Deferred Annuity  
Individual Variable Annuity  
Private Placement Variable Universal Life (Onshore)  
Individual ROP Term

## ***Excluded Products***

The following products are excluded by the regulation or based on the risk assessment findings:

Group Universal Life  
Group Variable Universal Life  
Group Fixed Annuity  
Group Variable Annuity  
Term  
Health  
Credit Life  
Credit Disability  
Property & Casualty

---

## **Systems**

The following systems are included in the AML monitoring procedures:

- Life Comm 86
- Vantage
- Navisys
- Master
- Presidential Annuity
- ULA
- Life Comm 90
- VFLEX
- CyberLife

The following systems are currently being monitored through the Compliance automated AML Alert Management System:

- Navisys
- Vantage



---

## General Information

**The following general information is applicable to ALL business units (Producer, New Business, Underwriting and POS) at ALL sites within the Domestic Life Companies.**

### ***RED FLAGS / SUSPICIOUS ACTIVITY INDICATORS***

#### **Producer**

- Customer shows little or no concern for the investment performance of the product, but a great deal of interest about the early termination features and seems to be knowledgeable about early surrender, loans, withdrawals, and free look periods
- Customer is reluctant to provide identifying information when purchasing the product, provides minimal or seemingly fictitious information
- Customer uses a deceased person's social security number or provides information that is inconsistent or appears suspicious
- Customer does not want to meet agent at residence or place of employment or who wants to meet during odd hours
- Customer pays initial premium with checks or wire transfers from the account of an unrelated (NOT the Owner, Payor, or Insured) third party
- Customer applies for policy from a distant location when comparable coverage can be obtained closer to home
- Customer accepts unfavorable underwriting conditions for his age or health
- Customer does not ask how much the product will cost, does not want to compare products based upon cost/benefit ratio and may offer to pay higher premium for speed and other accommodations
- Customer presents unusual or suspect personal or business identification documents
- Customer questions whether government report will be filed based upon transaction
- Customer has criminal record or is publicly associated with known felons
- Customer, their family, or close associates, are senior foreign political officials
- Customer has accounts in country identified as a tax haven
- Customer asks for details about or exception to policies/procedures that deter money laundering
- Applicant buy policies from several insurers in a short period of time

## **New Business / Underwriting**

- Purchase of an insurance product inconsistent with the consumer's needs or for an amount that is beyond his or her apparent means – unwilling to go through a needs analysis
- Unusual payment methods (Cash, Cash equivalent, money order, traveler's check, cashier's check, third party checks), Structured monetary instruments, overpayment of premium, checks drawn on agent account
- Early termination of a product (including free look period) especially at a cost to the customer
- Cash With Application (CWA) refund – directed to an unrelated third party
- Applicant not concerned about surrender cost, risks involved with the product, or interested in illustration of future benefits
- Applicant shows little concern for the investment performance of the product, but a great deal of interest in the early termination features and seems to be knowledgeable about early surrender, loans withdrawals and free look periods
- Applicant is reluctant to provide identifying information when purchasing the product, provides minimal or seemingly fictitious information
- Applicant uses multiple bank accounts to make payments or pays with numerous money sources to avoid the \$5,000 SAR reporting requirement
- The issue and underwriting of a covered product to a person in a jurisdiction whose government is on the blocked countries OFAC list, identified on FATF as a non-cooperative with international anti-money laundering principles or on FinCEN as warranting special measures due to money laundering concerns
- Applicant uses a deceased person's social security number or provides information that is inconsistent or appears suspicious
- Applicant pays with checks or wire transfers from the account of an unrelated third party
- Wire transfers to or from offshore banks, non-bank financial institutions or other financial intermediaries
- Applicant applies for a policy from a distant location when comparable coverage can be obtained closer to home
- Applicant accepts unfavorable underwriting conditions for his or her age or health
- Applicant does not ask how much the product will cost, does not want to compare products based upon cost/benefit ratio and may offer to pay higher premium for speed and other accommodations
- Applicant presents unusual or suspect personal or business identification documents
- Applicant questions whether a government report will be filed based upon transaction
- Applicant has criminal record or publicly associated with known felons
- Applicant, their family members, or close associates are senior foreign political officials
- Applicant has accounts in country identified as a tax haven
- Applicant requests information about or for an exception to Company policies and procedures that deter money laundering
- Applicant applies for or purchases multiple policies from several different insurers in a short period of time

## **Policyowner Services**

- Early termination of product (including free look period), especially at a cost (high surrender charge, etc) to the customer
- Refund check (Cash with Application, Premium Refund, Disbursement, etc) directed to an unrelated (NOT Owner, Payor, or Insured) third party
- Customer not concerned about surrender cost, risks involved with the product or interested in illustration of future benefits
- Transfer of the policy benefit or owner/beneficiary change to an apparently unrelated third party or charitable organization
- Customer shows little concern for the investment performance of the product, but a great deal of interest about the early termination features and seems to be knowledgeable about early surrender, loans, withdrawals and free look periods
- Customer prepays (or overpays) premiums and then borrows the maximum amount available or uses as collateral soon after purchasing the product
- Ownership of policy changed soon after policy issued
- Customer questions whether government report will be filed based upon transaction
- Customer asks for details about or exception to policies/procedures that deter money laundering
- Changes of address to foreign countries

## **Premium Processing**

- Unusual payment methods [Cash, Cash equivalent (money order, traveler's check, cashier's check, third party checks), Structured monetary instruments, overpayment of premium, checks drawn on agent's account]
- Premium Refund requested after overpayment
- Premium Refund directed to an unrelated (NOT Owner, Payor, or Insured) third party
- Customer prepays premiums and then borrows the maximum amount available or uses as collateral soon after purchasing the product
- Customer uses multiple bank accounts to make payments or pays with numerous money sources (e.g.: money order, cashier's check, third party check, cash, etc) to avoid the \$5,000 SAR reporting requirement
- Customer pays premium with check or wire transfer from the account of an unrelated third party
- Wire transfer to or from offshore banks, non-bank financial institutions, or other financial intermediaries

---

## ***Tax Haven Countries***

The following Countries and Jurisdictions have been identified by the Organisation for Economic Co-operation and Development (OECD) as uncooperative tax havens. These countries have not made commitments to transparency and effective exchange of information in tax matters. Listing was updated April 20, 2009, based on OECD April 2009 Report.

Andorra	Costa Rica	Netherlands Antilles
Anguilla	Dominica	Nevis
Antigua	Dominican Republic	Niue
Aruba	Gibraltar	Panama
Austria	Grenada	Philippines
Bahamas	Grenadines	Samoa
Bahrain	Guatemala	San Marino
Barbuda	Latvia thru Niue	Singapore
Belgium	Liberia	St. Kitts
Belize	Liechtenstein	St. Lucia
Bermuda	Luxembourg	St. Vincent
British Virgin Isles	Malaysia (Labuan)	Switzerland
Brunei	Marshall Islands	Turks & Caicos Islands
Canary Islands	Monaco	Uruguay
Cayman Islands	Montserrat	Vanuatu
Chile	Myanmar (Burma)	Western Samoa
Cook Islands	Nauru	

## ***OFAC Blocked Countries***

Balkans	Democratic Republic of the Congo	North Korea
Belarus	Iran	Sudan
Burma	Iraq	Syria
Cote d'Ivoire (Ivory Coast)	Liberia	Zimbabwe
Cuba		

---

## New Business and Underwriting

### ***IPO (Excluding Annuity) New Business Processing***

Based on the risk assessment, the following procedures are to be followed for **IPO (Excluding Annuity) New Business Processing**, to monitor 'Cash With Application' (CWA) initial premium payments received, refunds, and initial application review for individual life insurance products with cash value or investment features.

### **CWA Initial Premium Payment Review**

#### **Unacceptable forms of payment:**

- Cash
- Money Order
- Travelers Check
- Agent or Agency Check
- Foreign Check or Foreign Currency
- Check (Personal or Business) drawn on agent's account (A rare exception would be a situation when the agent is the payor – for example, he is purchasing insurance for his office personnel.)
- Third Party Check (remitter has no relation to policy or check is made payable to someone other than the Proposed Insured, Payor, Owner or Owner's business)
- Foreign Wire Transfer
- Personal Check that is:
  - ✓ Postdated
  - ✓ Stale – dated over 3 months
  - ✓ Not payable to AIGAG or American General (and doesn't fall under the exceptions for third party checks above)
  - ✓ Written amount and numeric amount differ by more than \$10.00

New Business and Treasury will not process any unacceptable forms of payment. Receipt of any of the above items should be rejected. New Business will notify the agent that an unacceptable form of payment has been received and New Business or Treasury will return the unacceptable payment to the client or to the agent for delivery to the client.

---

**Acceptable forms of payment:**

- Personal Check
- Business Check
- Insurance Company Check
- Trust Check (written on the Trust's account)
- Wire Transfer\*
- Bank Authorization
- Credit Card Authorization (for initial payment only – not acceptable in NJ, NY, PR)
- Cashier's Check\*\*

\*Originating from a domestic (United States) financial institution.

**NOTE: Foreign account wire transfers require further investigation by the Milwaukee Treasury Department.**

\*\*Cashier's Checks will be accepted when accompanied by the Source of Funds Certification Form (#AGLC103222), signed by an authorized representative of the issuing financial institution certifying that:

- The funds to purchase the check were taken directly from the customer's account at the financial institution issuing the check
- The check will be used by the customer to purchase a policy from American General
- The payor is a customer of the financial institution issuing the check

NOTE:

- The issuing financial institution must be located in the United States.
- A Cashier's Check may be issued by a financial institution who is also the policyowner
- If the required Source of Funds Certification Form is not received within 3 days of submission of the Application, the Cashiers Check will be returned.

New Business will follow standard procedures for processing acceptable forms of payment. For the vast majority of cases, the Owner, Payor, and Applicant are the same person.

This procedure applies to initial premium payments only. It does not affect transactions directly between the policyowner and the companies such as renewal premium, loan repayments, or payments to clear returned drafts or checks.

---

## **IPO Initial Application Review**

### **Underwriter Initial Application Review:**

Normal underwriter application verification procedures inherently review for Anti Money Laundering “Red Flags/Suspicious” activities such as:

- Suspicious or incomplete personal, business or trust identification documents.
- Applicant with criminal record or felony charges.
- Foreign account or address information, particularly in countries identified as tax havens or OFAC Blocked Countries.
- Product and face amount inconsistent with applicant’s needs and means. (Reference IOLI procedures.)
- Applicant reluctant to provide identifying information.
- Applicant who applied for or purchased multiple policies from several insurers in a short period of time or purchased a large single pay or lump sum policy when past patterns show the purchase of smaller payment products.

### **MIB:**

An MIB search is performed for only the proposed insured. If an MIB 011 hit code appears, Underwriter notifies Compliance via email and continues with underwriting. However, the case cannot be issued until Compliance notifies New Business regarding final disposition of the MIB hit.

### **OFAC (Office of Foreign Assets Control):**

Each morning Compliance receives a report listing the possible New Business OFAC hits. If Compliance is unable to verify the customer’s identity, an email will be sent to the New Business OFAC contact advising that the contract cannot be issued. Underwriting can continue, but the case cannot be issued until Compliance advises New Business of the final disposition of the OFAC hit.

Applicants with account or address information from a country identified on the OFAC Blocked Countries list are declined.

### **Required Action:**

If any of the above activities are identified and cause suspicion, the Underwriter is responsible to research and determine if policy should be declined. Such policies will be referred to Compliance on a case by case basis.

Foreign account information is reviewed by Treasury.

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

---

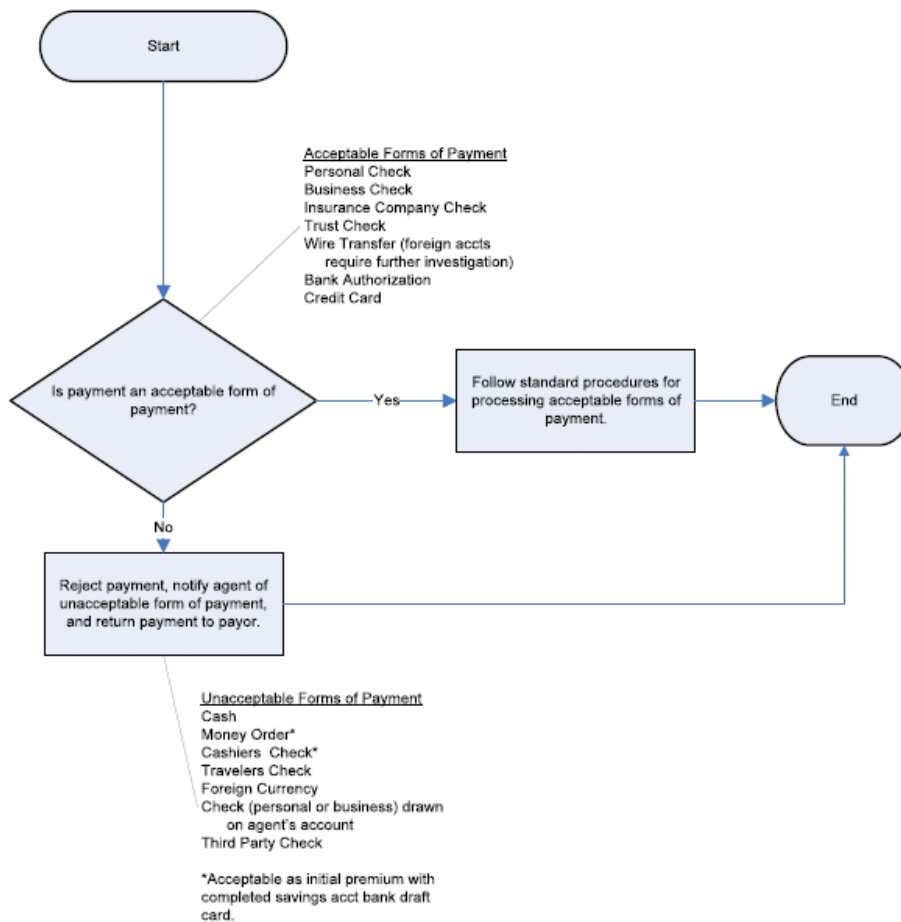
---

## CWA Refund Check

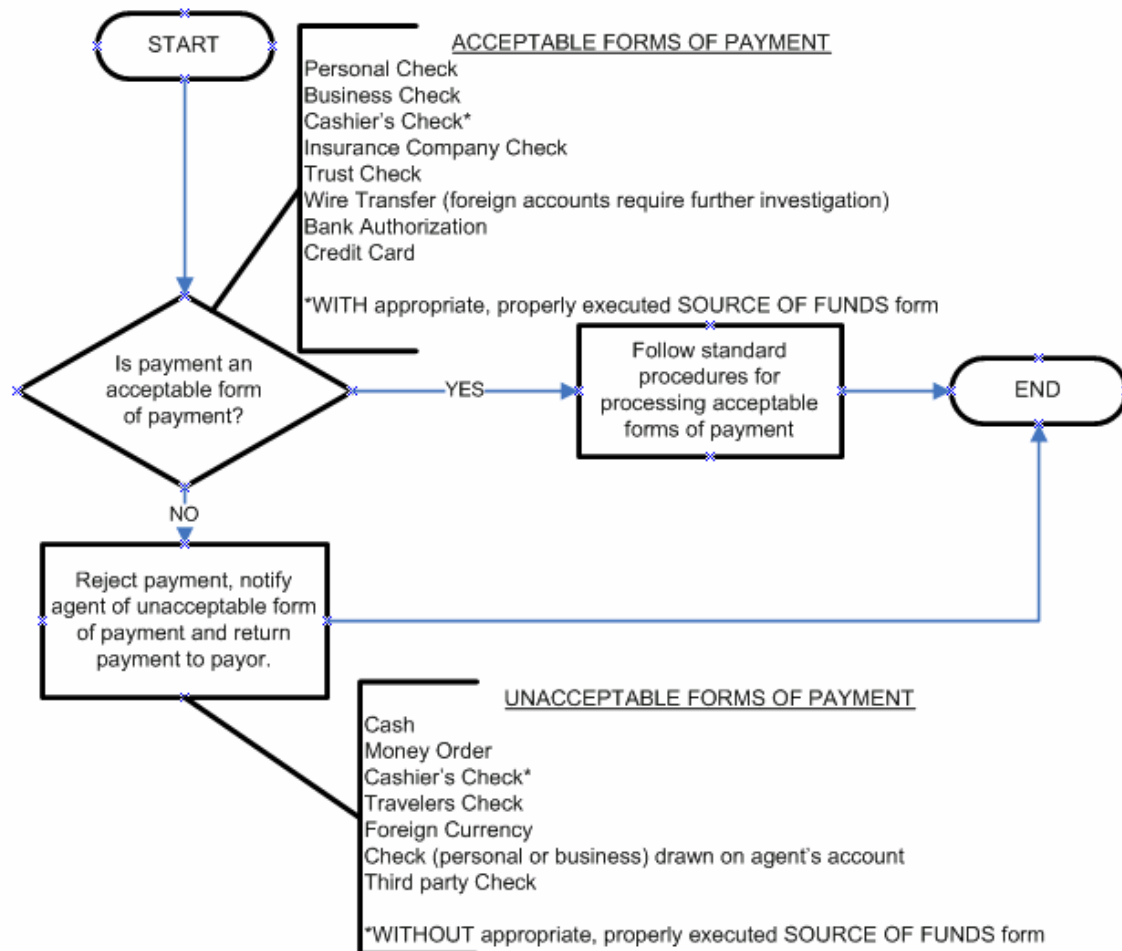
Refund checks are usually made payable to the policy owner and in some circumstances the payor. *(There are some circumstances in which the refund is made payable to someone other than the policyowner. An example would be list bill cases)* Any potential suspicious activity would have been previously investigated and reported when application was received. If refund is due to Not Taken or Cancellation within the free look period and the refund exceeds \$5,000, the refund will be completed and Compliance will be automatically notified through the Compliance Alert Management system.



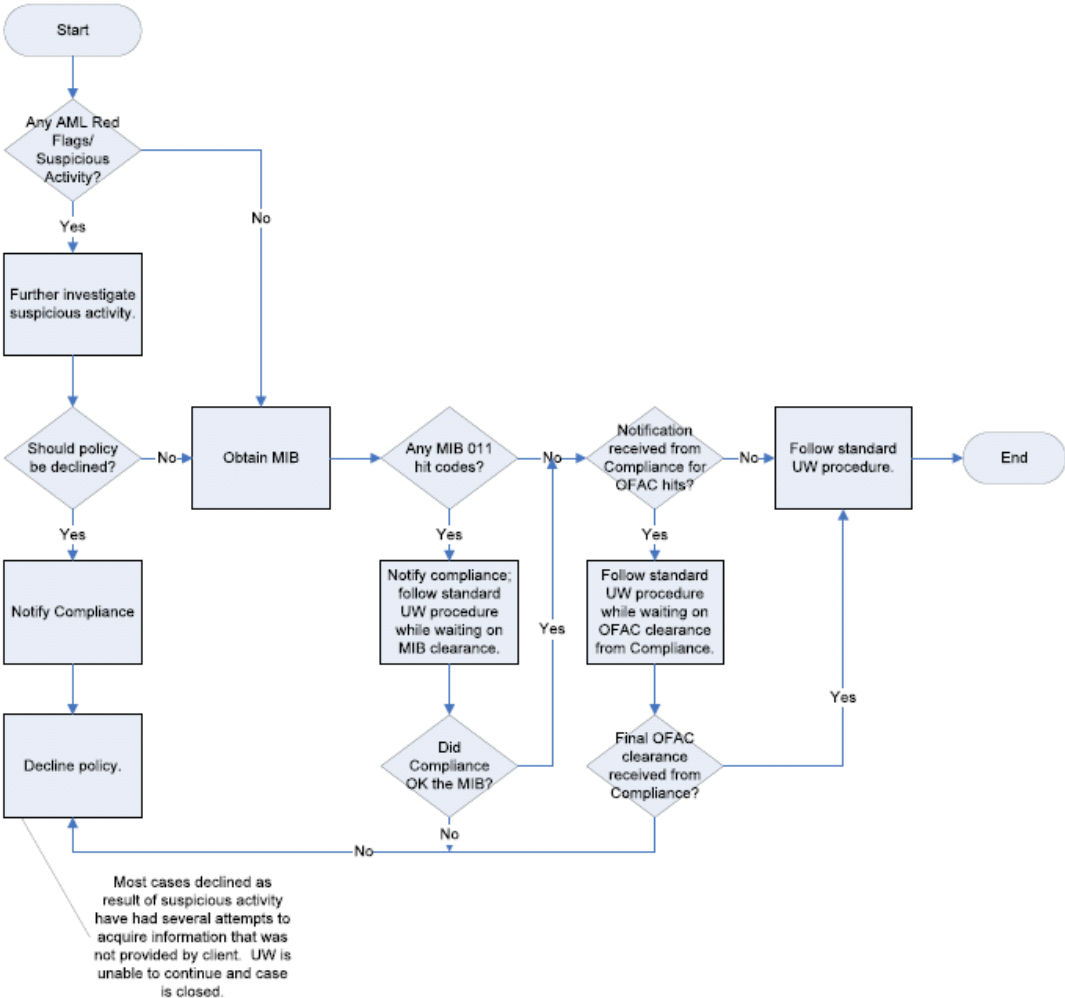
## AML – New Business – Cash with Application Initial Premium Payment Procedure



# AML – New Business CWA Initial Premium Payment Process



# AML – New Business – Underwriter Initial Application Review Procedure



---

## ***Houston Annuity New Business Processing***

Based on the risk assessment, the following procedures are to be followed to monitor CWA initial premium payments received, refunds, and initial application review for annuity products.

### **CWA Initial Premium Payment Review**

**(Also see AML – CWA –Unacceptable Payment Method Flowchart)**

#### **Unacceptable forms of payment:**

- Cash
- Money Order
- Cashiers Check\*
- Travelers Check
- Foreign Currency (including business and personal checks)
- Check (Personal or Business) drawn on agents account
- Third Party Check (excluding insurance company check)

**\*Acceptable for applicant only as initial premium when submitted with the appropriate, properly executed Source of funds form.**

New Business and Treasury will not process any unacceptable forms of payment. Receipt of any of the above items should be rejected. New Business will notify the agent that an unacceptable form of payment has been received and New Business or Treasury will return the unacceptable payment to the payor.

#### **Acceptable forms of payment:**

- Personal Check
- Business Check
- Insurance Company Check
- Trust Check
- Wire Transfer (foreign account wires are not permitted)
- Bank Authorization (debit)

New Business will follow standard procedures for processing acceptable forms of payment.

For the majority of cases the Purchaser, Owner, Annuitant and Payee are the same person.

---

## **CWA and 1035/ Trustee Transfer Refund Check under Free look/NTO**

Refund checks are made payable to the contract owner only unless the purchase involved a 1035 or Trustee Transfer. Under a 1035 or Trustee Transfer the funds are returned to the source to avoid adverse tax consequences to the client. Suspicious activity could occur if we receive a request to send the funds to an unrelated 3<sup>rd</sup> party. Any suspicious activity will be referred to Annuity Compliance for further investigation and referred to Shared Services Compliance. Each case will be documented on an AML Referral Checklist and entered on the AML Activity log.

### **Annuity Initial Application Review**

Processors prescreen all applications and are trained to identify AML red flags. Any suspicious applications will be referred to Annuity Compliance for review.

#### **OFAC:**

Each morning Compliance receives a report listing the possible New Business OFAC hits for contracts issued on the Vantage system. If Compliance is unable to verify the customer's identity, an email will be sent to the New Business OFAC contact advising that the contract cannot be issued.

Applicants with account or address information from a country identified on the OFAC Blocked Countries list are declined.

#### **Required Action:**

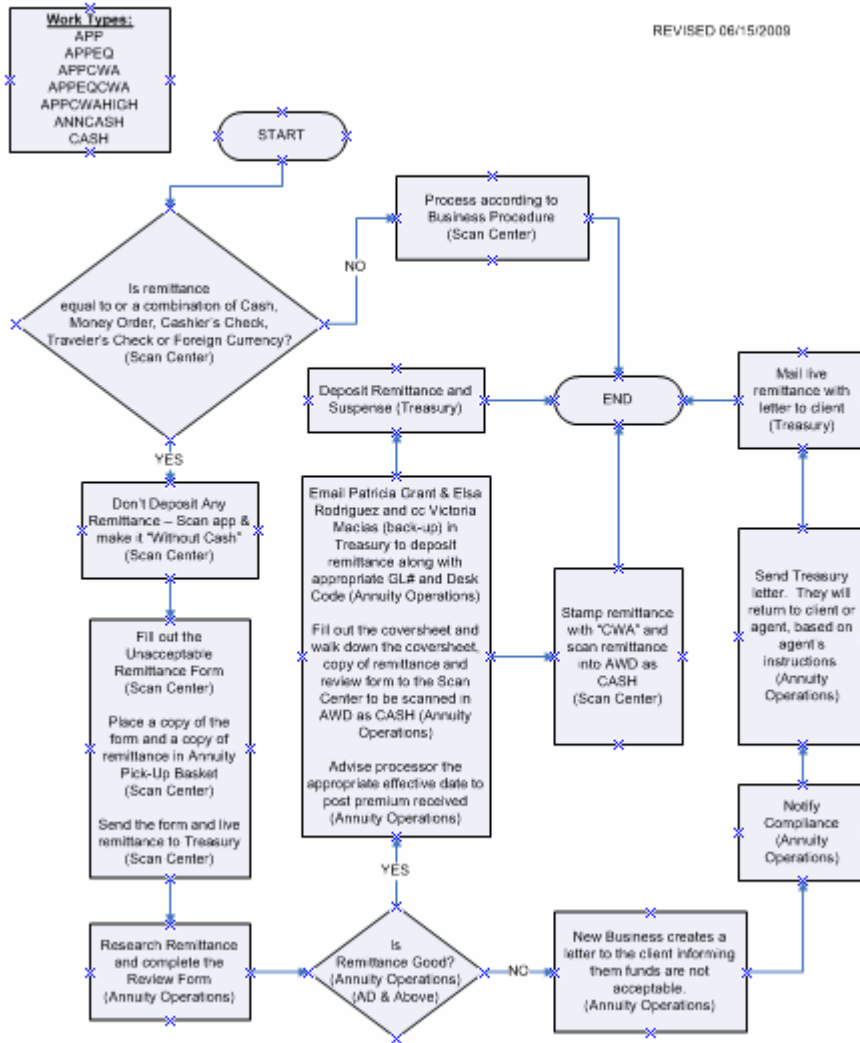
If any of the above activities are identified and cause suspicion, Annuity Compliance is responsible to research and determine if contract should be declined. Such contracts will be referred to Shared Service Compliance for suspicious activity reporting. Each case will be documented on an AML Referral Checklist and entered on the AML Activity log.

Foreign account information is reviewed by Treasury.

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

# Houston Annuity AML – Unacceptable Payment Method

REVISED 06/15/2009



---

# **Houston Annuity Unacceptable Remittance**

Amount: \_\_\_\_\_

Policy Number: \_\_\_\_\_

Date Received: \_\_\_\_\_

Action:

1. Fill in the above information.
2. Place a copy of this form and a copy of the remittance in the Annuity Pick-Up basket.
3. Send this form and the remittance to Treasury.

---

# Houston Annuity Service Center Unacceptable Remittance Review Form

Remittance Type: \_\_\_\_\_

Amount: \_\_\_\_\_

Policy Number: \_\_\_\_\_

Comments: \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Approved By: \_\_\_\_\_

Date: \_\_\_\_\_

**\*\*\*\*\*PROCESSING NOTE\*\*\*\*\***

**PROCESS WITH EFFECTIVE DATE: \_\_\_\_\_**



---

## ***Wilmington Annuity New Business Processing***

Based on the risk assessment, the following procedures are to be followed to monitor CWA initial premium payments received, refunds, and initial/underwriter contract review for annuity insurance products.

### **CWA Initial Premium Payment Review**

#### **Unacceptable forms of payment:**

- Cash
- Money Order
- Cashiers Check\*
- Travelers Check
- Foreign Currency
- Check (Personal or Business) drawn on agents account
- Third Party Check

New Business and Treasury will not process any unacceptable forms of payment. Receipt of any of the above items should be rejected. New Business will notify the agent that an unacceptable form of payment has been received and New Business or Treasury will return the unacceptable payment to the purchaser of the annuity.

#### **Acceptable forms of payment:**

- Personal Check
- Business Check
- Insurance Company Check
- Trust Check
- Wire Transfer (foreign account wire transfers require further investigation)
- Bank Authorization
- Credit Card
- Cashier's Check (WITH the properly executed Source of Funds form)

New Business will follow standard procedures for processing acceptable forms of payment.

### **Refund of Premium within Free Look Period**

Refund checks are made payable to the person who provided the premium check (purchaser of annuity). Any potential suspicious activity would have been previously investigated and reported when application was received. If refund is due to Cancellation within the free look period and the refund exceeds \$5,000, refund approval will be completed in AWD by individual with approval authority and referred to the AML liaison. The AML liaison will log case on AML Activity log, complete AML Referral Checklist and forward to Compliance.

---

## Wilmington Annuity Initial Application Review

### Underwriter Initial Application Review:

Normal underwriter application verification procedures inherently review for Anti Money Laundering “Red Flags/Suspicious” activities such as:

- Suspicious or incomplete personal, business or trust identification documents.
- Foreign account or address information, particularly in countries identified as tax havens or OFAC Blocked Countries.
- Product and face amount inconsistent with applicant’s needs and means. (Reference IOLI procedures.)
- Applicant reluctant to provide identifying information.
- Applicant who applied for or purchased multiple policies from several insurers in a short period of time or purchased a large single pay or lump sum policy when past patterns show the purchase of smaller payment products.

### OFAC:

For large New Business enrollments, Compliance receives a report listing the possible New Business OFAC hits. If Compliance is unable to verify the customer’s identity, an email will be sent to the New Business OFAC contact advising that the contract cannot be issued. Underwriting can continue, but the case cannot be issued until Compliance advises New Business of the final disposition of the OFAC hit.

All other annuity applications are manually run through the Accuity IFACS website by the Wilmington New Business team. If a hit is found, the case is referred to Houston Compliance.

Applicants with account or address information from a country identified on the OFAC Blocked Countries list are declined.

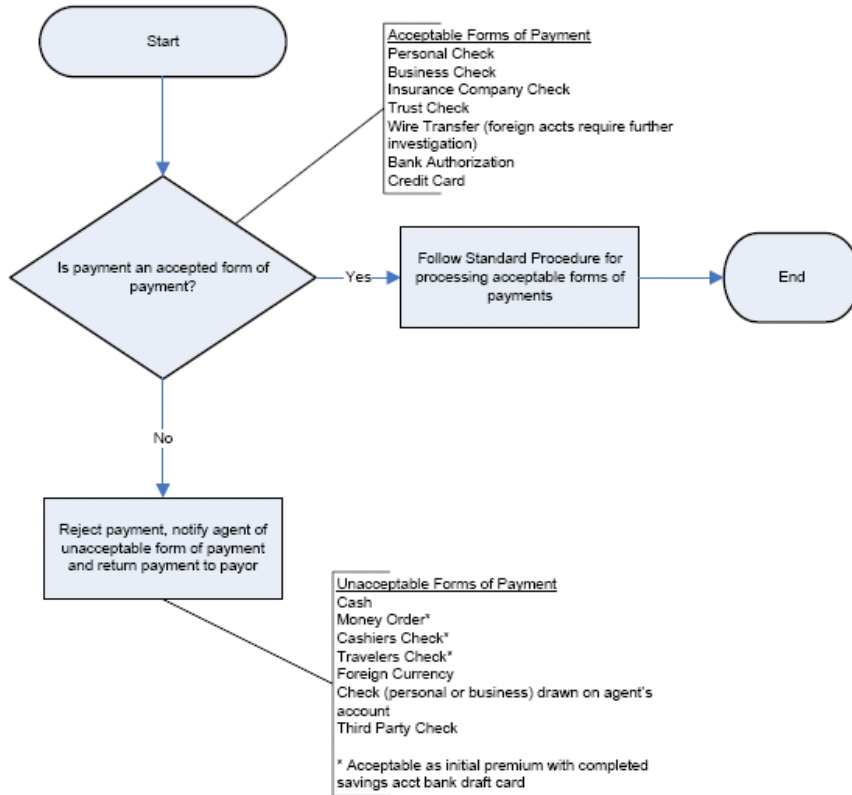
### Required Action:

If any of the above activities are identified and cause suspicion, the Underwriter is responsible to research and determine if policy should be declined. The case should be referred to the AML liaison who will log case on AML Activity log, complete AML Referral Checklist and forward to Compliance.

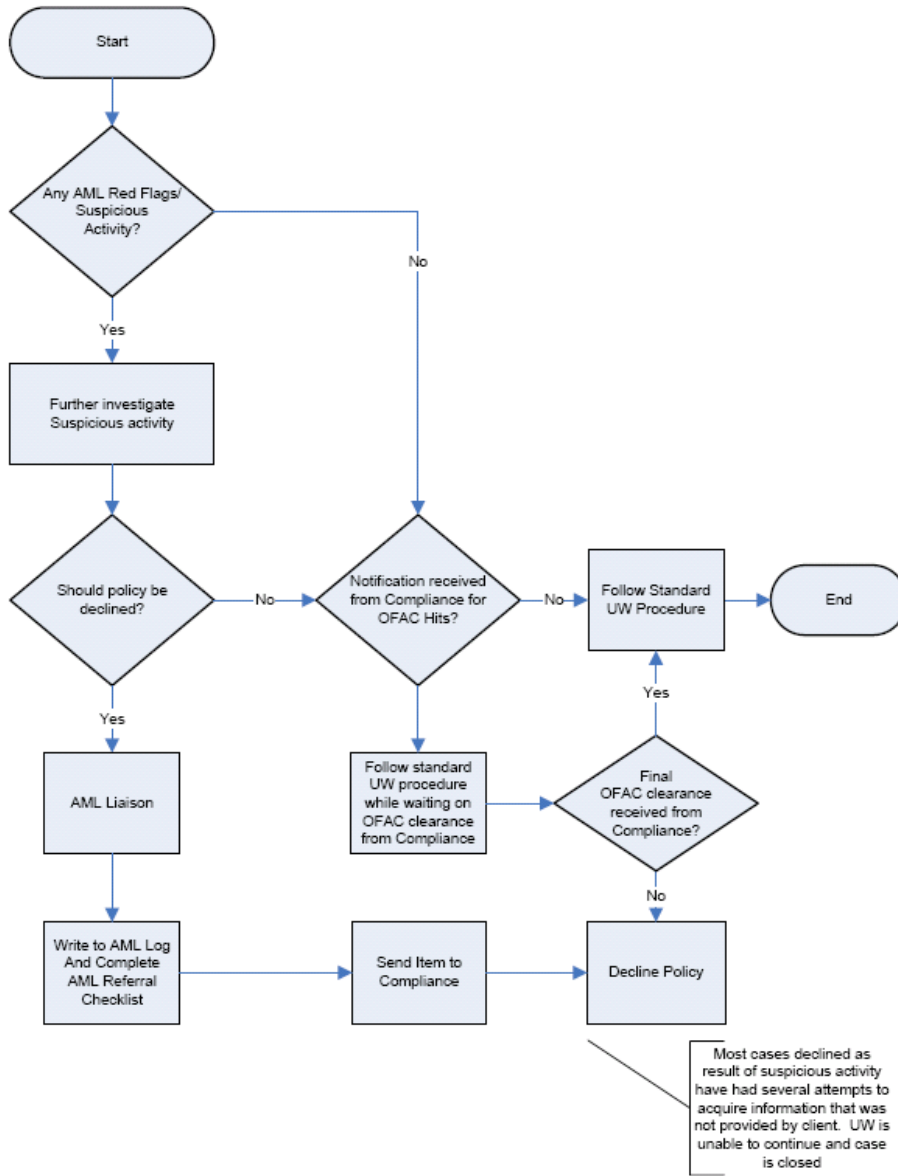
Foreign account information is reviewed by Treasury.

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

**Wilmington Annuity**  
**AML - New Business – Cash with Application**  
**Initial Premium Payment Procedure**



# Wilmington Annuity AML – New Business – Initial Application Review Procedure





---

**WILMINGTON ANNUITY ADMINISTRATION  
ANTI-MONEY LAUNDERING (AML)  
REFERRAL CHECKLIST**

This cover page should be used when referring an AML case to Compliance for review.  
Be sure this entry is also added to the Anti-Money Laundering Activity Log.

DATE REFERRED: \_\_\_\_\_ REFERRED BY: \_\_\_\_\_

SITE/DEPARTMENT: \_\_\_\_\_

Place checkmark in box for AML Activity being reported.

New Business Activity	Premium & Unusual Payment Activity	POS Activity
New Business Initial Premium	Exception Payments	Beneficiary Change
Refund of Premium Within Free Look Period		Ownership Change
Red Flag - Initial Review		Address Change
<b>Red Flag – Underwriter Review</b>		

System Affected: \_\_\_\_\_

Contract Number: \_\_\_\_\_

Client Name: \_\_\_\_\_

Brief description of AML activity being reported (attach any supporting documentation):

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

For Compliance Use Only:

Assigned to: \_\_\_\_\_

SAR submitted \_\_\_\_\_

Date: \_\_\_\_\_

No SAR required \_\_\_\_\_

---

## **EBS New Business Processing**

Based on the risk assessment, the following procedures are to be followed to monitor CWA refunds and initial application review for individual life insurance products with cash value or investment features.

### **Refund Check**

Refund checks are made payable to the policy owner only. Any potential suspicious activity would have been previously investigated and reported when application was received. If refund is due to Not Taken or Cancellation within the free look period and the refund exceeds \$1,000, refund approval will be completed in AWD by individual with approval authority and referred to the AML liaison. The AML liaison will log case on AML Activity log, complete AML Referral Checklist and forward to Compliance.

### **EBS Initial Application Review**

#### **Underwriter Initial Application Review:**

Normal underwriter application verification procedures inherently review for Anti Money Laundering "Red Flags/Suspicious" activities such as:

- Suspicious or incomplete personal, business or trust identification documents.
- Applicant with criminal record or felony charges.
- Foreign account or address information, particularly in countries identified as tax havens or OFAC Blocked Countries.
- Product and face amount inconsistent with applicant's needs and means.
- Applicant reluctant to provide identifying information.
- Applicant who applied for or purchased multiple policies from several insurers in a short period of time or purchased a large single pay or lump sum policy when past patterns show the purchase of smaller payment products.

#### **OFAC:**

Each morning Compliance receives a report listing the possible New Business OFAC hits. If Compliance is unable to verify the customer's identity, an email will be sent to the New Business OFAC contact advising that the contract cannot be issued. Underwriting can continue, but the case cannot be issued until Compliance advises New Business of the final disposition of the OFAC hit.

Applicants with account or address information from a country identified on the OFAC Blocked Countries list are declined.

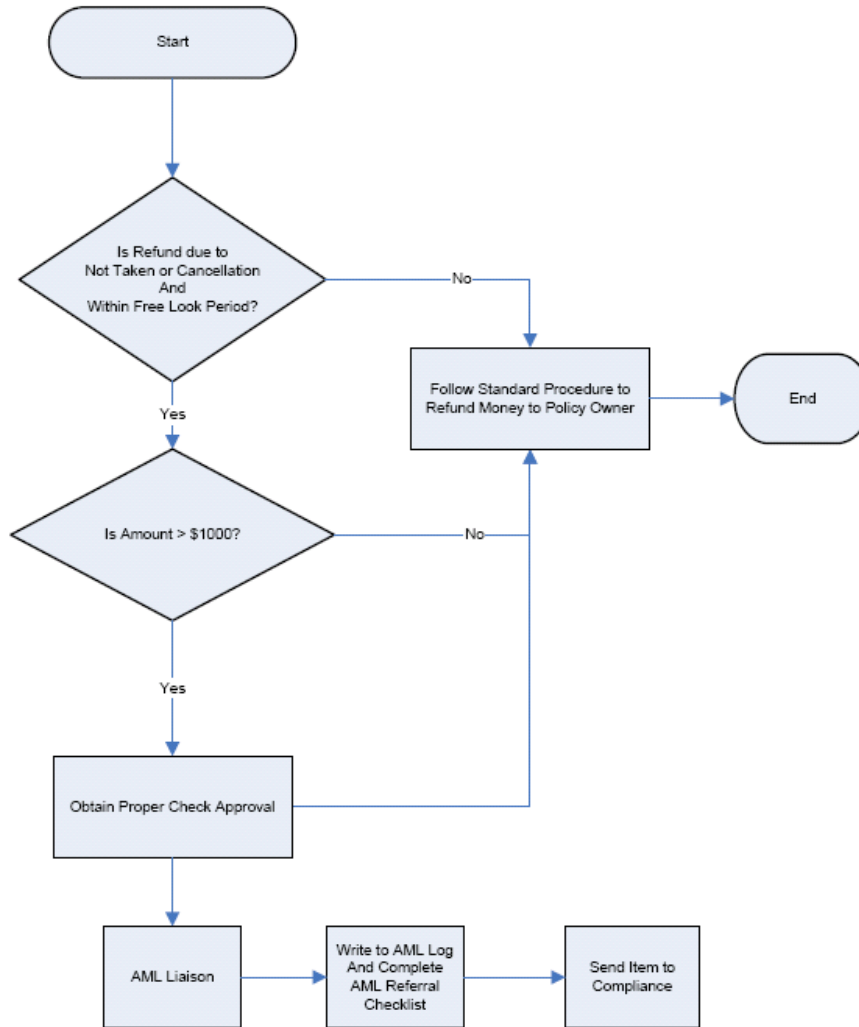
#### **Required Action:**

If any of the above activities are identified and cause suspicion, the Underwriter is responsible to research and determine if policy should be declined. The case should be referred to the AML liaison who will log case on AML Activity log, complete AML Referral Checklist and forward to Compliance.

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

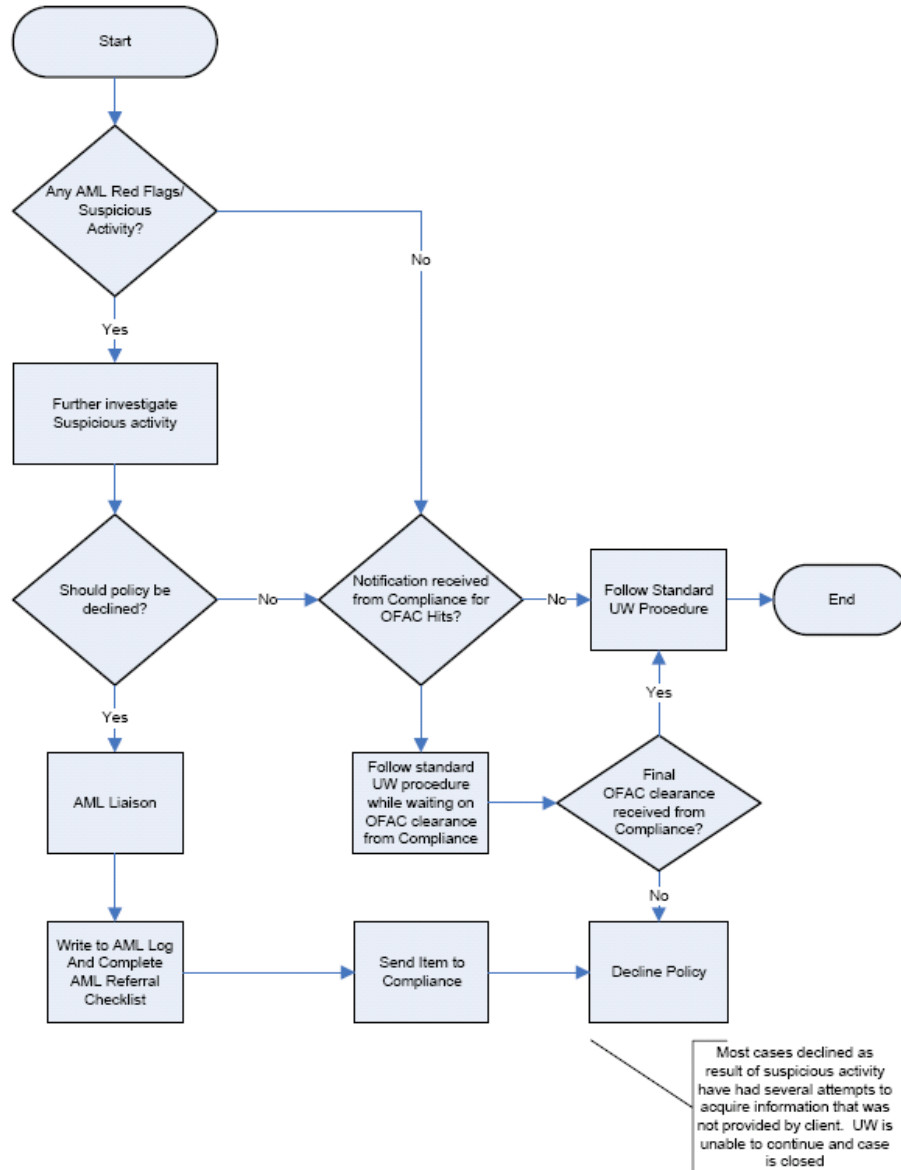
---

## **AML – EBS - New Business – Cash with Application Refund Check Procedure**





## AML – EBS - New Business – Initial Application Review Procedure



AML EBS Procedures.vsd Thursday, August 24, 2006

version 1.0



# EMPLOYEE BENEFIT SOLUTIONS ANTI-MONEY LAUNDERING (AML) REFERRAL CHECKLIST

This cover page should be used when referring an AML case to Compliance for review. Be sure this entry is also added to the Anti-Money Laundering Activity Log.

DATE REFERRED: \_\_\_\_\_ REFERRED BY: \_\_\_\_\_

SITE/DEPARTMENT: \_\_\_\_\_

Place checkmark in box for AML Activity being reported.

New Business Activity	Premium & Unusual Payment Activity	POS Activity
New Business Refund Check	Premium Refund	Not Taken Option (NTO)
Red Flag - Initial Review		
Red Flag - Underwriter Review		

System Affected: \_\_\_\_\_

Policy Number: \_\_\_\_\_

Client Name: \_\_\_\_\_

Brief description of AML activity being reported (attach any supporting documentation):

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

For Compliance Use Only:

Assigned to: \_\_\_\_\_  
SAR submitted \_\_\_\_\_

Date: \_\_\_\_\_  
No SAR required \_\_\_\_\_

---

## **AGLA New Business Processing**

Based on the risk assessment, the following procedures are to be followed to monitor new business refund checks for declined or retired applications and initial underwriter review for individual insurance products with cash value or investment features.

### **Underwriter Initial Application Review**

Normal underwriter application verification procedures inherently review Anti Money Laundering “Red Flags/Suspicious” activities such as:

- Suspicious or incomplete personal, business or trust identification documents.
- Foreign account or address information, particularly in countries identified as tax havens or OFAC Blocked Countries.
- Product and face amount inconsistent with applicant’s needs and means.
- Applicant reluctant to provide identifying information; provides minimal or seemingly fictitious information.
- Applicant with criminal record or felony charge.
- Applicant who applied for or purchased multiple policies (3 or more) from several direct life insurers in a short period of time (1 year or less).
- Applicant applies for a policy from a distant location when comparable coverage can be obtained closer to home.
- Applicant, their family members, or close associates are senior foreign political officials.
- Applicant requests information about or for an exception to Company policies and procedures that deter money laundering.

Applications of \$100,000 and greater are checked through the Insurance Activity Index at MIB. All applicant information is checked through the OFAC check. If information cannot be verified through OFAC, a letter is sent to the applicant requesting two forms of identification. Acceptable forms of identification are noted in this letter.

If there is a questionable foreign address of the primary proposed insured or owner, item should be noted on the Anti Money Laundering Activity Log, referred to Team Lead, Supervisor or Manager who then refers to Compliance.

Case does not proceed unless questionable information is satisfactorily resolved. Applicants with account or address information from an OFAC Blocked Country are declined.

If any of the above activities are identified and cause suspicion, the Underwriter is responsible to fully research and determine if policy should be declined. Suspicious items should be added on the Anti Money Laundering Activity Log, referred to Team Lead, Supervisor or Manager who then refers to Compliance.

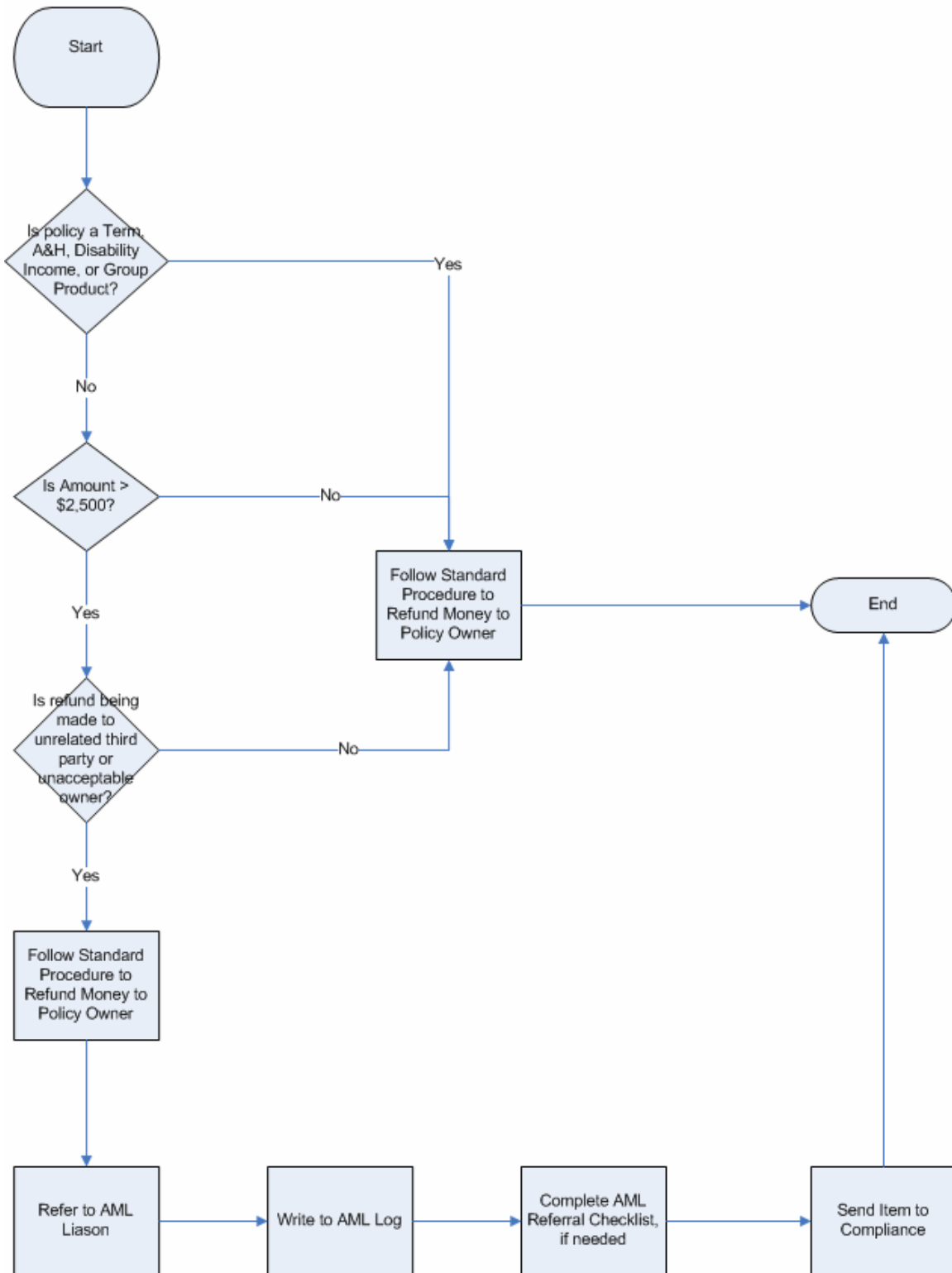
---

## **New Business Refund Check for Declined or Retired Applications**

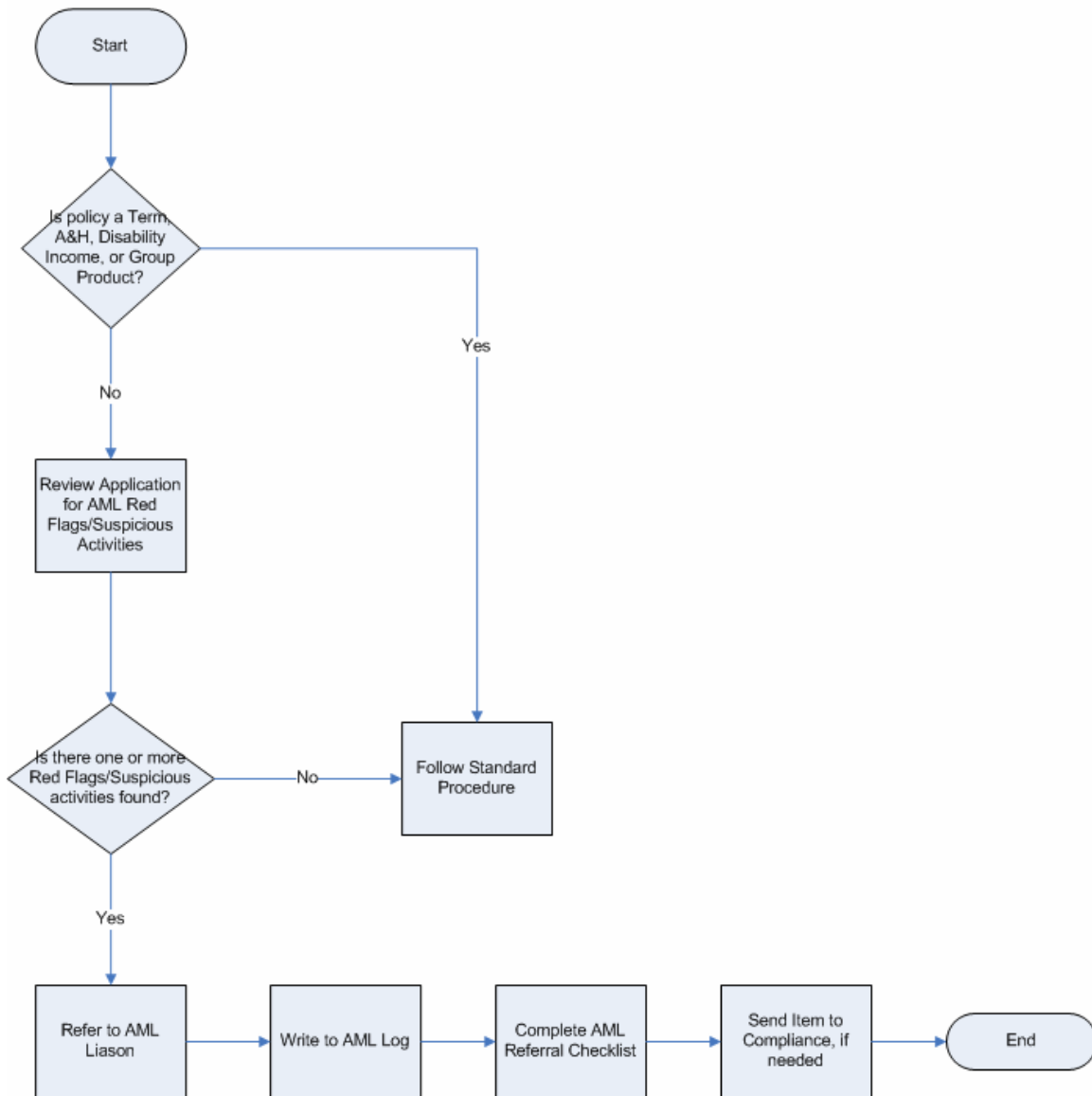
Under automatic procedures, refund checks are made payable to the policy owner only. Occasionally, a request to refund to payor is received and would be processed manually. Current procedures if ownership is questioned and no response – application would be declined and premium refunded. Any potential suspicious activity would be investigated and reported during the underwriting process.

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

# AML New Business Refund Check Procedure



## AML New Business Underwriter Review Procedure







## ANTI-MONEY LAUNDERING (AML) REFERRAL CHECKLIST

This cover page should be used when referring an AML case to Compliance for review. Be sure this entry is also added to the Anti-Money Laundering Activity Log.

DATE REFERRED: \_\_\_\_\_ REFERRED BY: \_\_\_\_\_

SITE/DEPARTMENT: \_\_\_\_\_

Place checkmark in box for AML Activity being reported.

New Business Activity	Premium & Unusual Payment Activity	POS Activity
Refund Check	Unusual Payment Method	Beneficiary Change
Red Flag – Underwriter Review	Exception Processing	Ownership Change
	History/Pattern Review	Address Change
		Surrender – Full or Partial Loan

System Affected: \_\_\_\_\_

Policy Number: \_\_\_\_\_

Client Name: \_\_\_\_\_

Brief description of AML activity being reported (attach any supporting documentation):

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Has AWD been noted about AML referral? \_\_\_\_\_

For Compliance Use Only:

Assigned to: \_\_\_\_\_

SAR submitted \_\_\_\_\_

Date: \_\_\_\_\_

No SAR required \_\_\_\_\_

---

## Policyowner Services (POS)

### IPO (excluding Annuity) POS (including EBS)

Based on the risk assessment, the following procedures are to be followed to monitor transactions for suspicious activity:

#### Title Changes

##### Owner & Beneficiary Change

- Was request denied by Legal due to unacceptable documentation?
  - Yes
    - Refer to AML Liaison
  - No
    - Process Title Change according to Business Rules
    - Is product Term, A&H, Disability Income, or Group?
      - Yes – Process – no further action required
      - No
        - Is Face > \$100,000 & Policy inforce < 6 months?
          - Yes – refer to AML Liaison
          - No – process according to Business Rules

##### Address Change

- Process address change according to Business Rules
  - Is product Term, A&H, Disability Income, or Group?
    - Yes - Process – no further action required
    - No
      - Is the address change to an Uncooperative Tax Haven country or a country on the OFAC list?
        - Yes – refer to AML Liaison
        - No – process according to Business Rules

---

## Disbursements

### Not Taken Offer (NTO)

- Process NTO according to Business Rules
  - Is product Term, A&H, Disability Income, or Group?
    - Yes – Process – no further action required
    - No - Is NTO > \$5,000
      - No – Process – no further action required
      - Yes - Is NTO payment being refunded made within the last 3 months?
        - Yes – refer to AML Liaison
        - No – Is NTO check being sent to an OFAC or Tax Haven Country?
          - Yes – refer to AML Liaison
          - No – Process – no further action required

### Surrender, Partial, & PDF/Prepay Withdrawal

- Process Disbursement according to Business Rules
  - Is Disbursement > \$5,000 & policy has been in force < 1 year?
    - No – Process – no further action required
    - Yes – Is Disbursement a 1035 Exchange or Rollover?
      - Yes – Process – no further action required
      - No – Premium/PDF/Prepay Dump-In > \$5,000 in last 3 months?
        - Yes – refer to AML Liaison
        - No – Is Surrender Charge > 25% of cash value?
          - Yes – refer to AML Liaison
          - No – Is Disbursement being sent to Tax Haven or OFAC country?
            - Yes – refer to AML Liaison
            - No – Process – no further action required

### Loan

- Process Loan according to Business Rules
  - Is Loan > \$5,000?
    - No – Process – no further action required
    - Yes – An evidence of Premium Dump-In in last 3 months?
      - Yes – refer to AML Liaison
      - No – Have there been multiple Loans & Loan Payments in the past year?
        - Yes – refer to AML Liaison
        - No – Has a Collateral Assignment been made in the last 3 months?
          - Yes – refer to AML Liaison
          - No – Is Loan being sent to a Tax Haven or OFAC country?
            - Yes – refer to AML Liaison
            - No – Process – no further action required

## **Premium Payments**

- Lockbox Exception Payments & Non-Lockbox Premiums
  - Process Payment Transaction according to Business Rules
  - Was the Premium paid by US funds via Personal Check, Business Check or Trust Check?
    - Yes – Process – no further action required
    - No – Was the Premium paid in Cash, Foreign Currency, or paid by Agent?
      - Yes – refer to AML Liaison
      - No – Is payment > \$1,000?
        - No – Process – no further action required
        - Yes – refer to AML Liaison

## **Premium Refund**

- Process Refund Transaction according to Business Rules
- Is product Term, A&H, Disability Income, or Group?
  - Yes – Process – no further action required
  - No – Is Refund > \$5,000?
    - No – Process – no further action required
    - Yes – Was Refund payment being refunded made within the last 3 months?
      - Yes – refer to AML Liaison
      - No – Is Refund check being sent to OFAC or Tax Haven country?
        - Yes – refer to AML Liaison
        - No – Process – no further action required

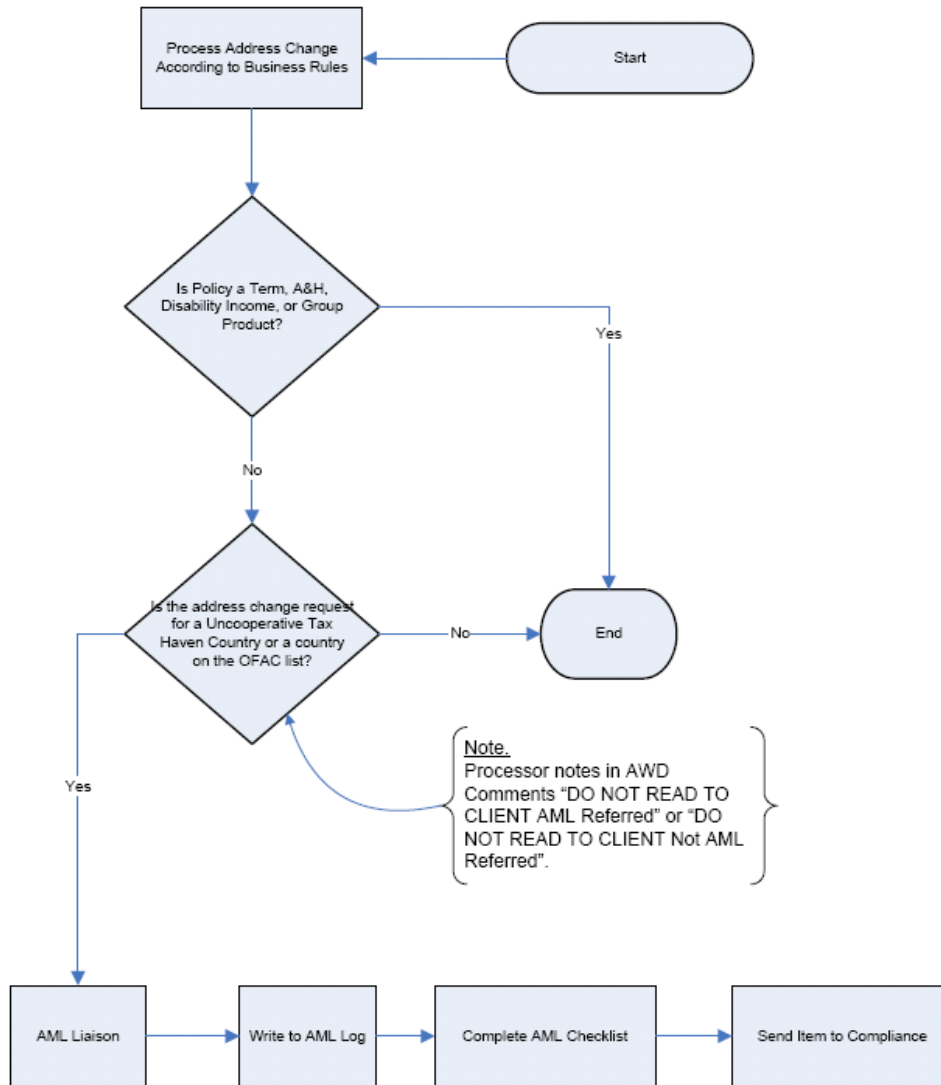
## **AML Liaison**

AML Liaison should do the following with items referred to them:

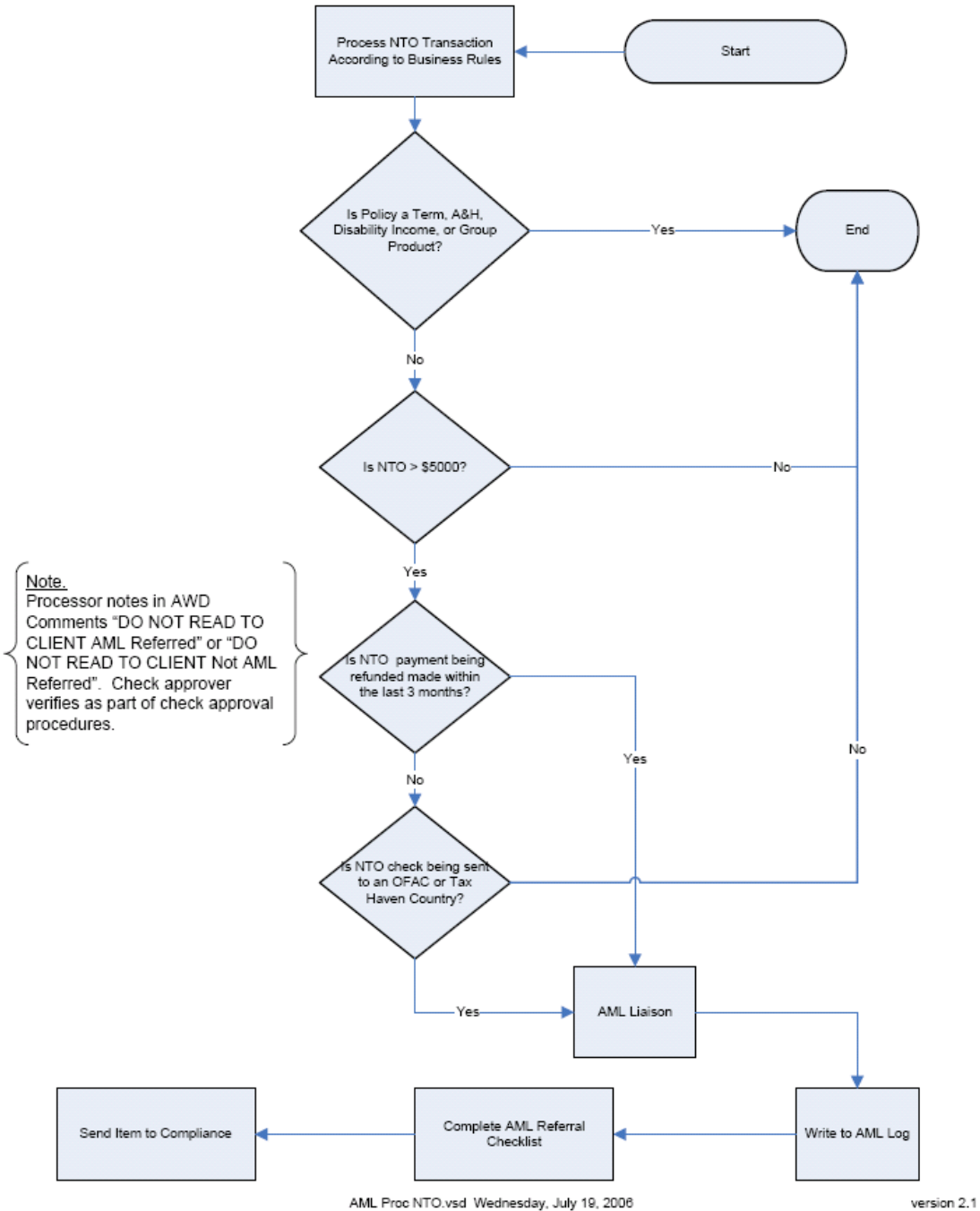
- Write to AML Log
- Complete AML Referral Checklist
- Send item to Compliance

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

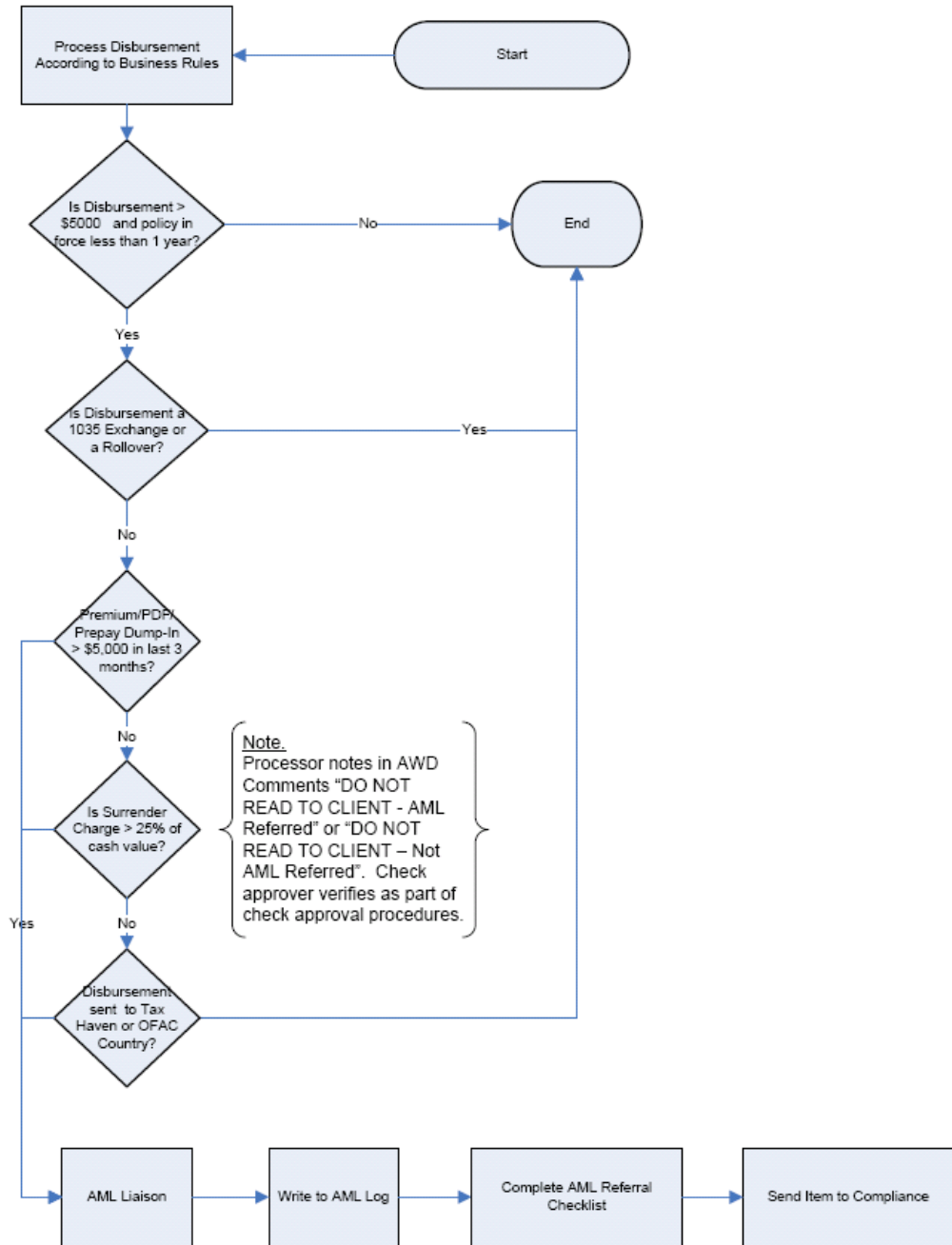
## AML – Address Change Procedures



## AML – NTO Procedures



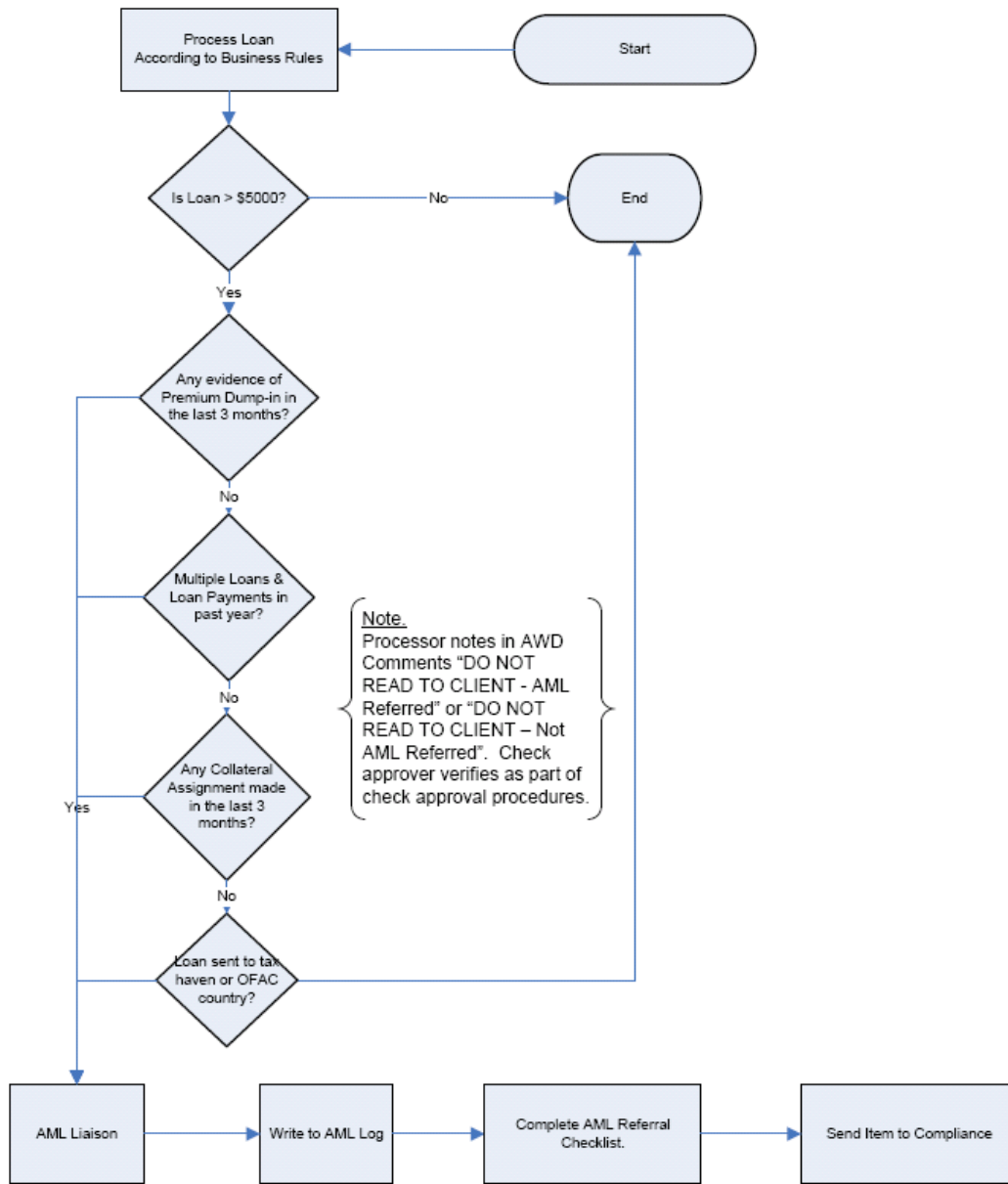
## AML – Disbursements – Surrenders, Partial and PDF/Prepay W/D Procedures



AML Proc - Disbursements - Surrenders and Partials.vsd Wednesday, July 19, 2006

version 2.0

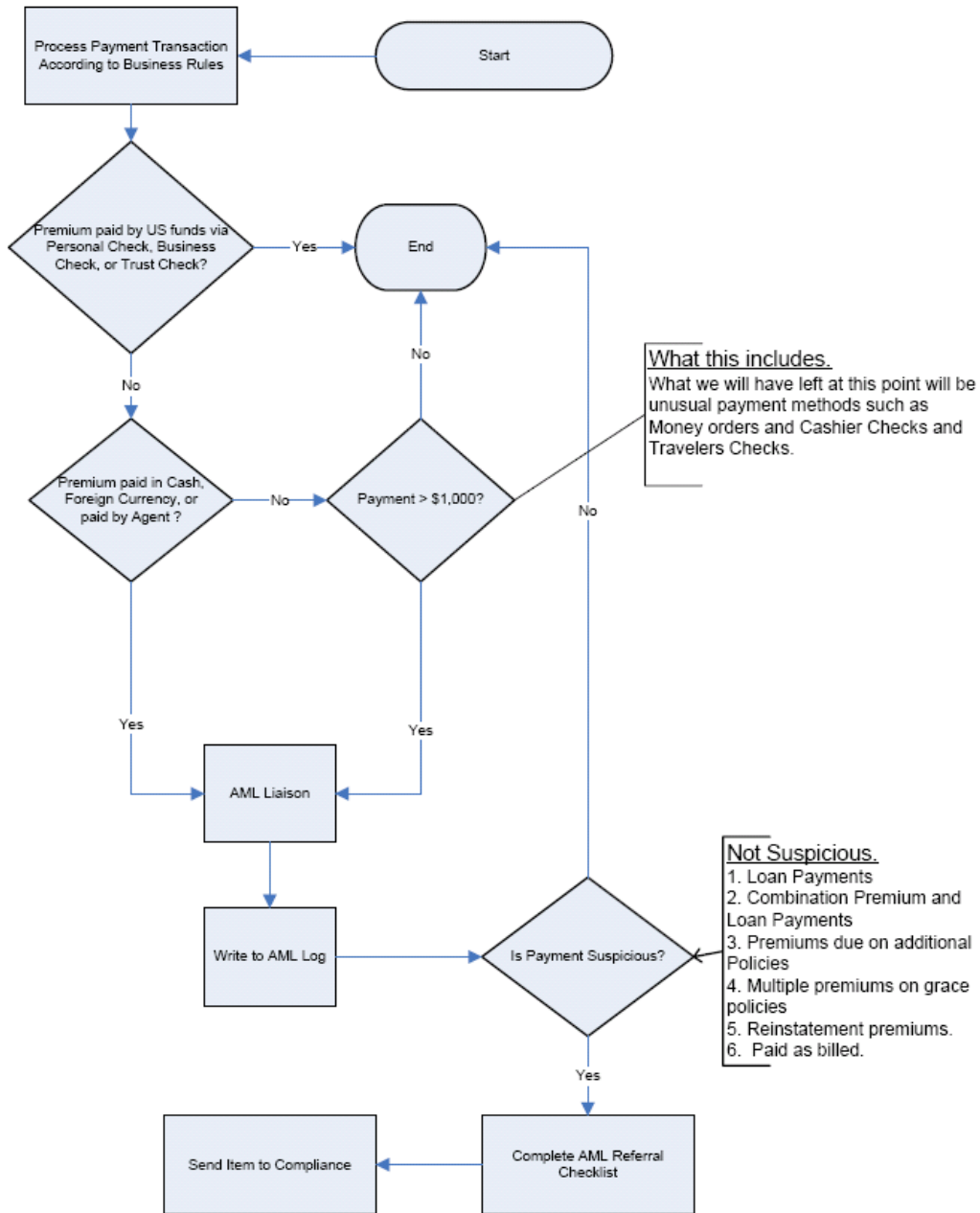
## AML – Disbursements – Loan Procedures



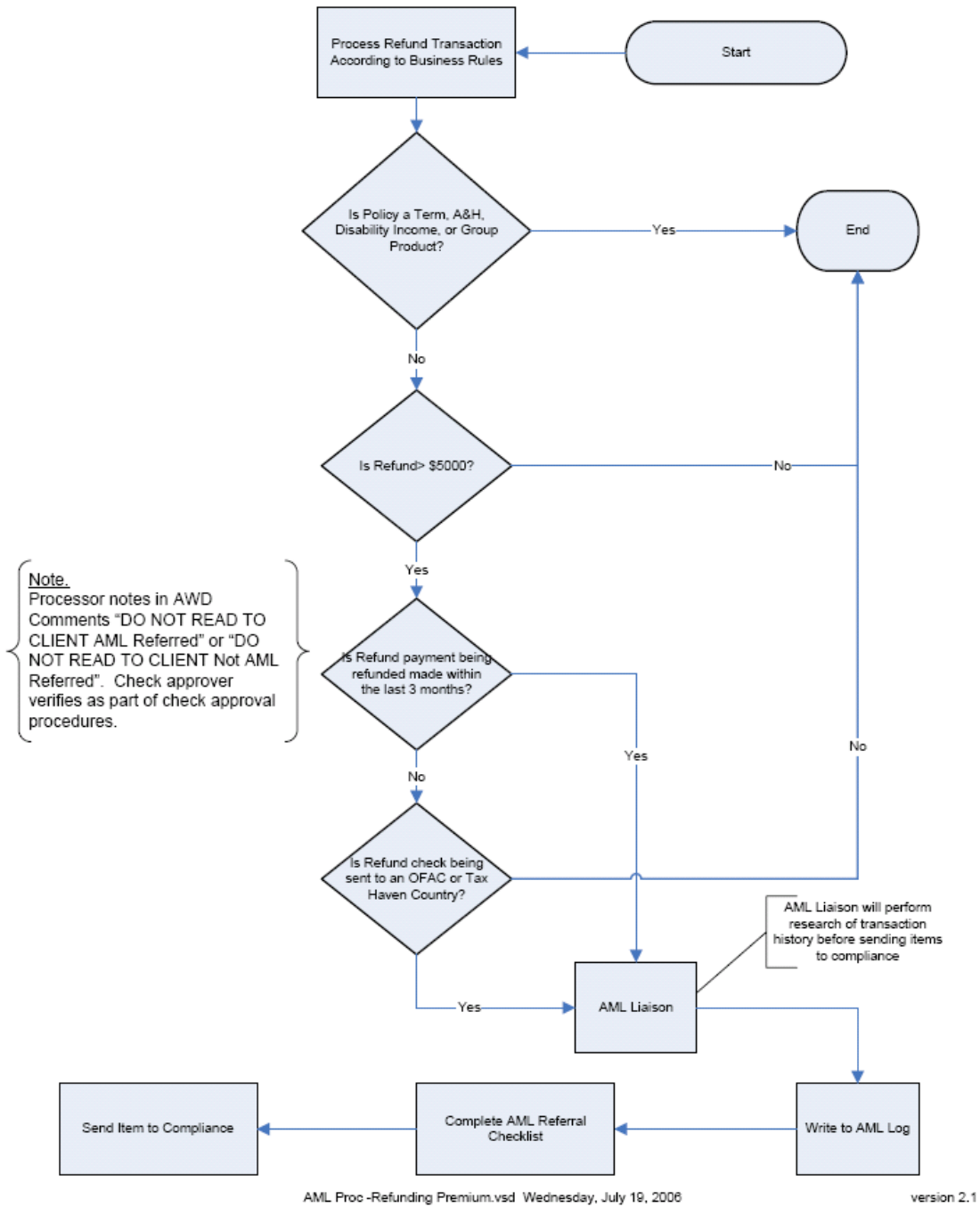




## AML – Lockbox Exception Payments & Non-Lockbox Premium Procedures



## AML – Premium Refund Procedures





## ANTI-MONEY LAUNDERING (AML) REFERRAL CHECKLIST

This cover page should be used when referring an AML case to Compliance for review. Be sure this entry is also added to the Anti-Money Laundering Activity Log.

DATE REFERRED: \_\_\_\_\_ REFERRED BY: \_\_\_\_\_

SITE/DEPARTMENT: \_\_\_\_\_

Place checkmark in box for AML Activity being reported.

New Business Activity	Premium & Unusual Payment Activity	POS Activity
CWA Initial Premium	Not Accepted Payment Form	Beneficiary Change
CWA Refund Check	Exception Processing	Ownership Change
Red Flag - Initial Review	Lump Sum Payment	Address Change
Red Flag - Underwriter Review	Premium Refund	Not Taken Option (NTO)
		Surrender – Full or Partial Loan

System Affected: \_\_\_\_\_

Policy Number: \_\_\_\_\_

Client Name: \_\_\_\_\_

Brief description of AML activity being reported (attach any supporting documentation):

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

For Compliance Use Only:

Assigned to: \_\_\_\_\_

SAR submitted \_\_\_\_\_

Date: \_\_\_\_\_

No SAR required \_\_\_\_\_

---

## **Houston Annuity Policyowner Services**

Based on the risk assessment, the following procedures are to be followed to monitor transactions for suspicious activity:

### **Disbursements**

#### **Not Taken Offer (NTO)**

- Process NTO/Freelook Transaction according to Business Rules
- Is Refund being made to a 3<sup>rd</sup> Party?
  - No – Process – no further action required
  - Yes – refer to Annuity Compliance
- Is Refund check being sent to an OFAC or Tax Haven Country?
  - No – Process – no further action required
  - Yes – refer to Annuity Compliance

#### **Premium Refund, Premium Paid in Excess of Contract**

- Process Refund Transaction according to Business Rules
- Is Refund being made to a 3<sup>rd</sup> Party?
  - No – continue process
  - Yes – refer to Annuity Compliance
- Is Refund check being sent to an OFAC or Tax Haven Country?
  - No – complete process
  - Yes – refer to Annuity Compliance

#### **Surrenders, Partial Surrenders, & Systematic Withdrawal**

- Process Disbursement according to Business Rules
- Is Disbursement in excess of free-out or systematic withdrawal amount?
  - No – Process – no further action required
  - Yes – Is Disbursement a 1035 Exchange or Rollover?
    - Yes – Process – no further action required
    - No – Is Disbursement within 1<sup>st</sup> 6 months of issue?\*
- Yes – refer to Annuity Compliance if other Red Flags exist.
- No – Is Disbursement being sent to a Tax Haven or OFAC country?
  - No – Process – no further action required
  - Yes – refer to Annuity Compliance

**\*Review of all disbursement amounts is conducted. Client may take a 10% Free Amount in the first year.**

---

## **Title Changes**

### **Address/Owner & Beneficiary Change**

- Process Change according to Business Rules
- Is the change request for an Uncooperative Tax Haven Country or a country on the OFAC list?
  - No – Process – no further action required
  - Yes – refer to Annuity Compliance

### **Periodic Payments – Change of Payee**

- Annuity Processor to Pre-Screen & Complete according to Business Rules
- Is the Payee change to unknown 3<sup>rd</sup> Party or a Tax Haven or OFAC country?
  - No – Process – no further action required
  - Yes – refer to Annuity Compliance

---

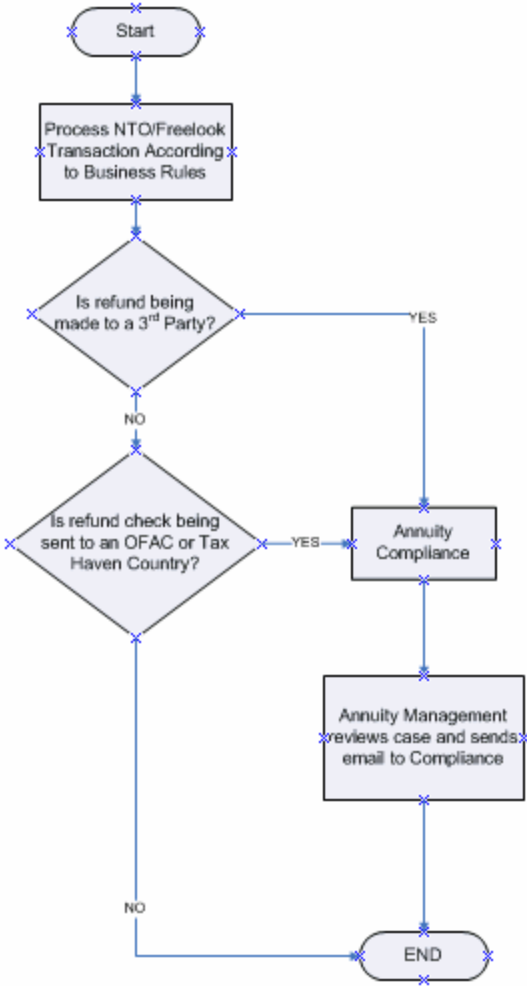
## **Annuity Compliance**

Annuity Compliance will do the following with items referred to them:

- Research transaction
- Write to AML Log
- Complete AML Referral Checklist
- Send item to Compliance

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

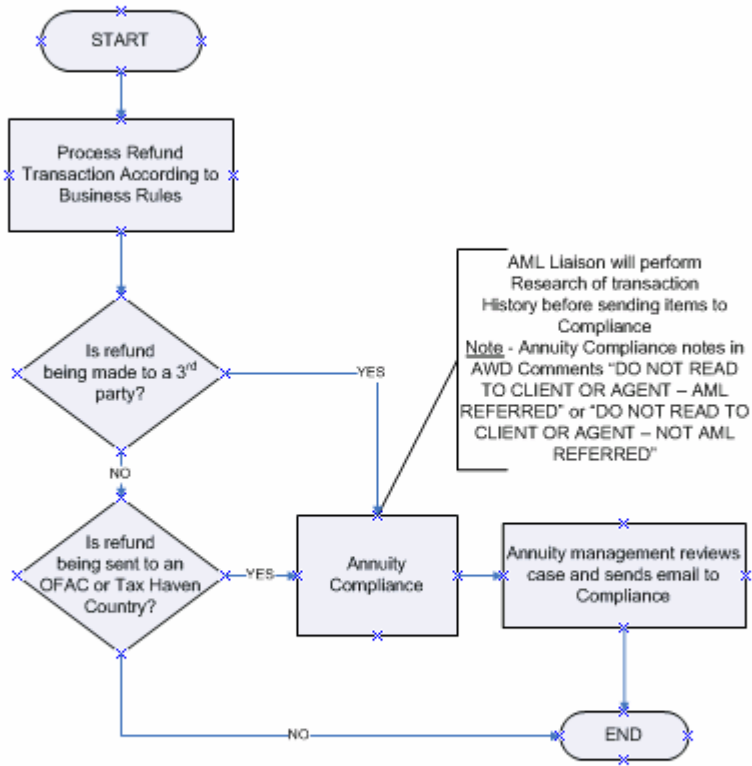
# Houston Annuity AML – NTO/FreeLook Procedure



REVISED 4/29/2009

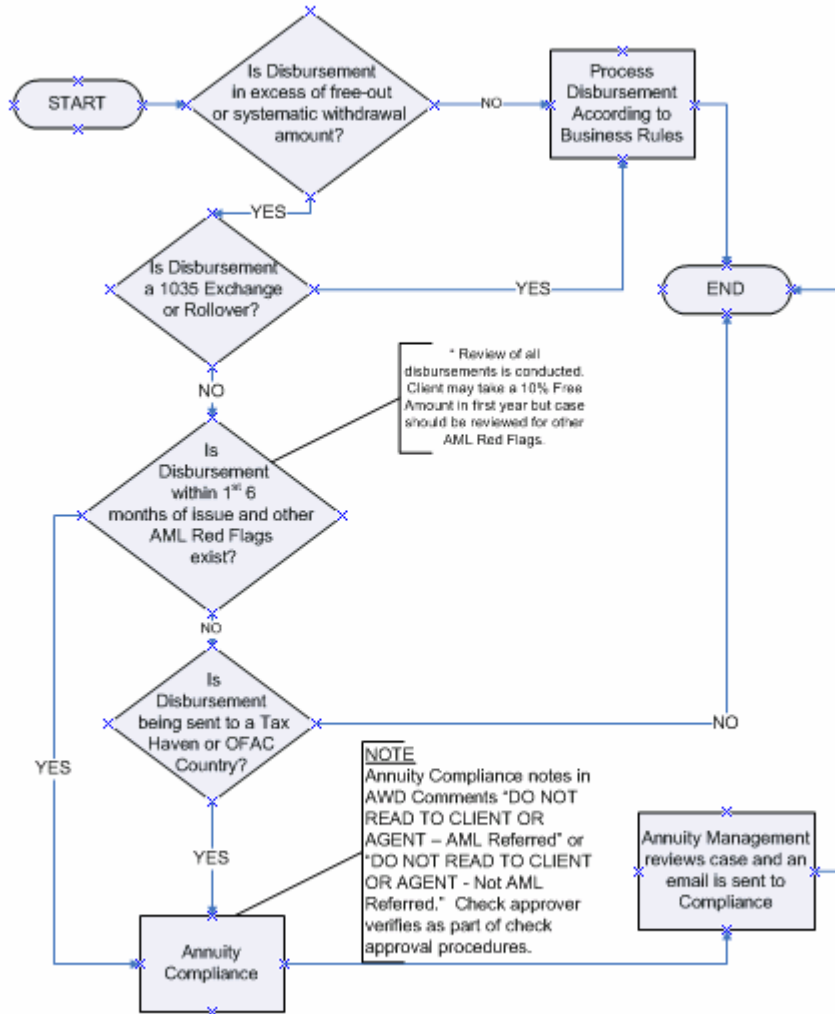


# Houston Annuity Premium Refund Procedure – Premium Paid in Excess of Contract



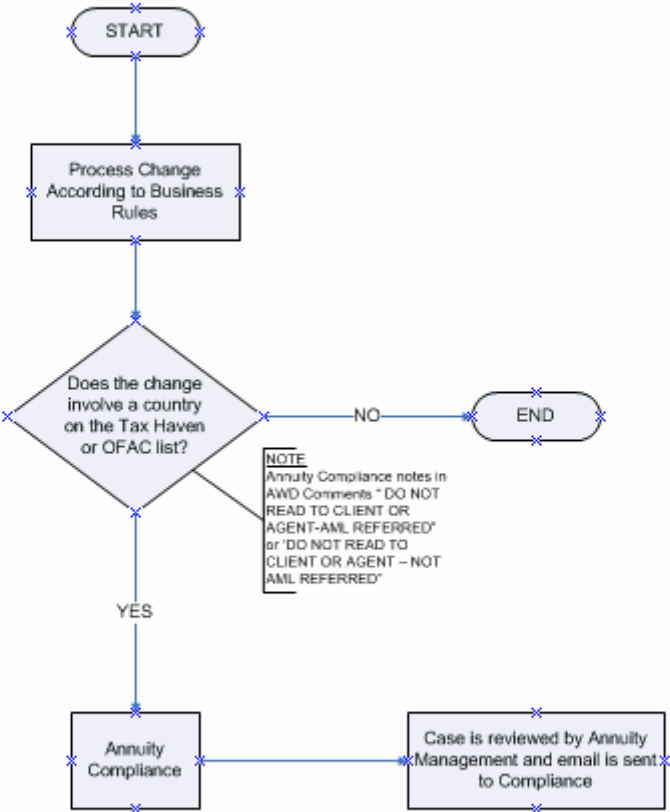
Revised 04-26-2009

## Houston Annuity AML – Surrenders, Partial Surrenders and Systematic Withdrawal



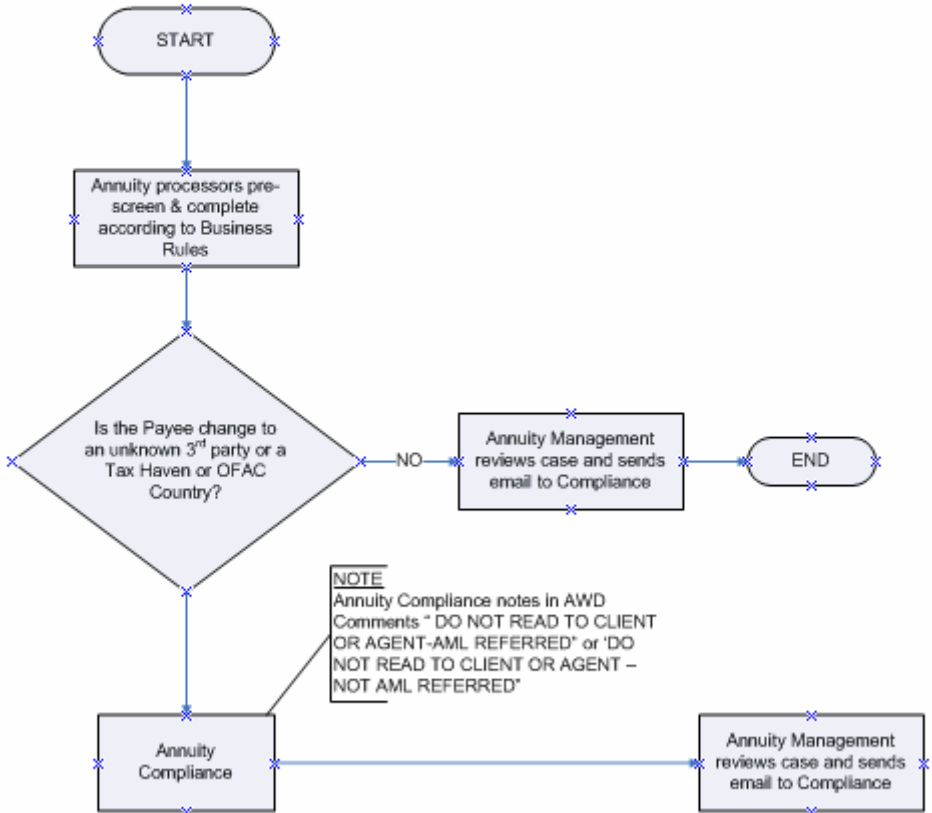
Revised 4/29/09

# Houston Annuity AML – Address/Owner & Beneficiary Change Procedures



Revised 04-29-2009

# Houston Annuity AML – Periodic Payment – Change of Payee



Revised 04-26-2009

## ***Wilmington Annuity Policyowner Services***

Based on the risk assessment, the following procedures are to be followed to monitor transactions for suspicious activity:

### **Disbursements**

#### **Refund of Premium within Free Look Period**

- Process Refund Transaction According to Business Rules
- Is Refund > \$5,000?
  - No – Process – no further action required
  - Yes – Is Refund check being sent to a Tax Haven or OFAC country?
    - No – Process – no further action required
    - Yes – refer to AML Liaison

#### **Lockbox Exception Payments & Non-Lockbox Premium Procedures**

- Process Payment Transaction According to Business Rules
- Was Premium paid by US funds via Personal Check, Business Check, or Trust Check?
  - Yes – Process – no further action required
  - No – Was Premium paid in Cash, Foreign Currency, or paid by Agent?
    - Yes – refer to AML Liaison
    - No – Is payment > \$1,000?
      - No – Process – no further action required
      - Yes – refer to AML Liaison

### **Title Changes**

#### **Address Change**

- Process Address Change according to Business Rules
- Is the address change requested for an Uncooperative Tax Haven Country or an OFAC country?
  - No – Process – no further action required
  - Yes – refer to AML Liaison

#### **Owner & Beneficiary Changes**

- Was request denied by Legal due to unacceptable documentation?
  - Yes – refer to AML Liaison
  - No – Process Title Change according to Business Rules
- Is Contract < 6 months old?
  - No – Process – no further action required
  - Yes – refer to AML Liaison

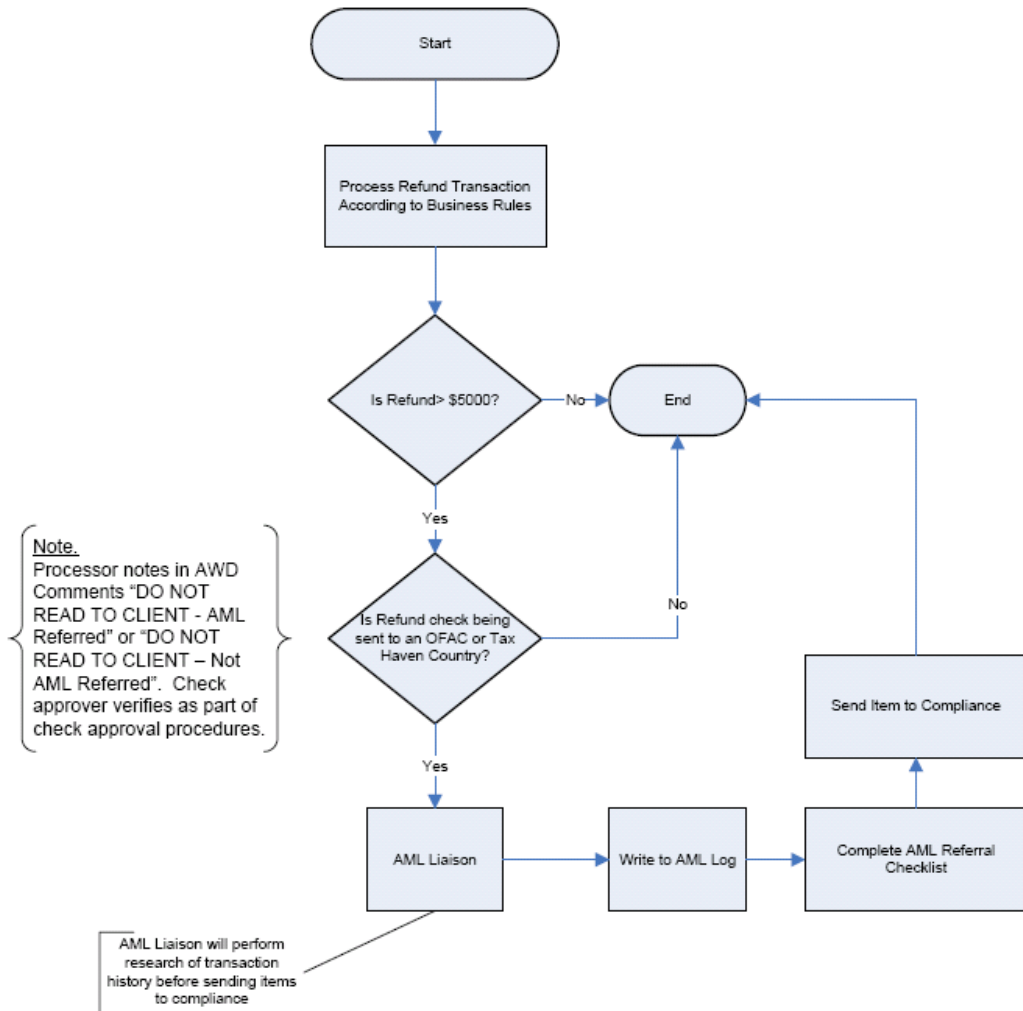
## **AML Liaison**

AML Liaison should do the following with items referred to them:

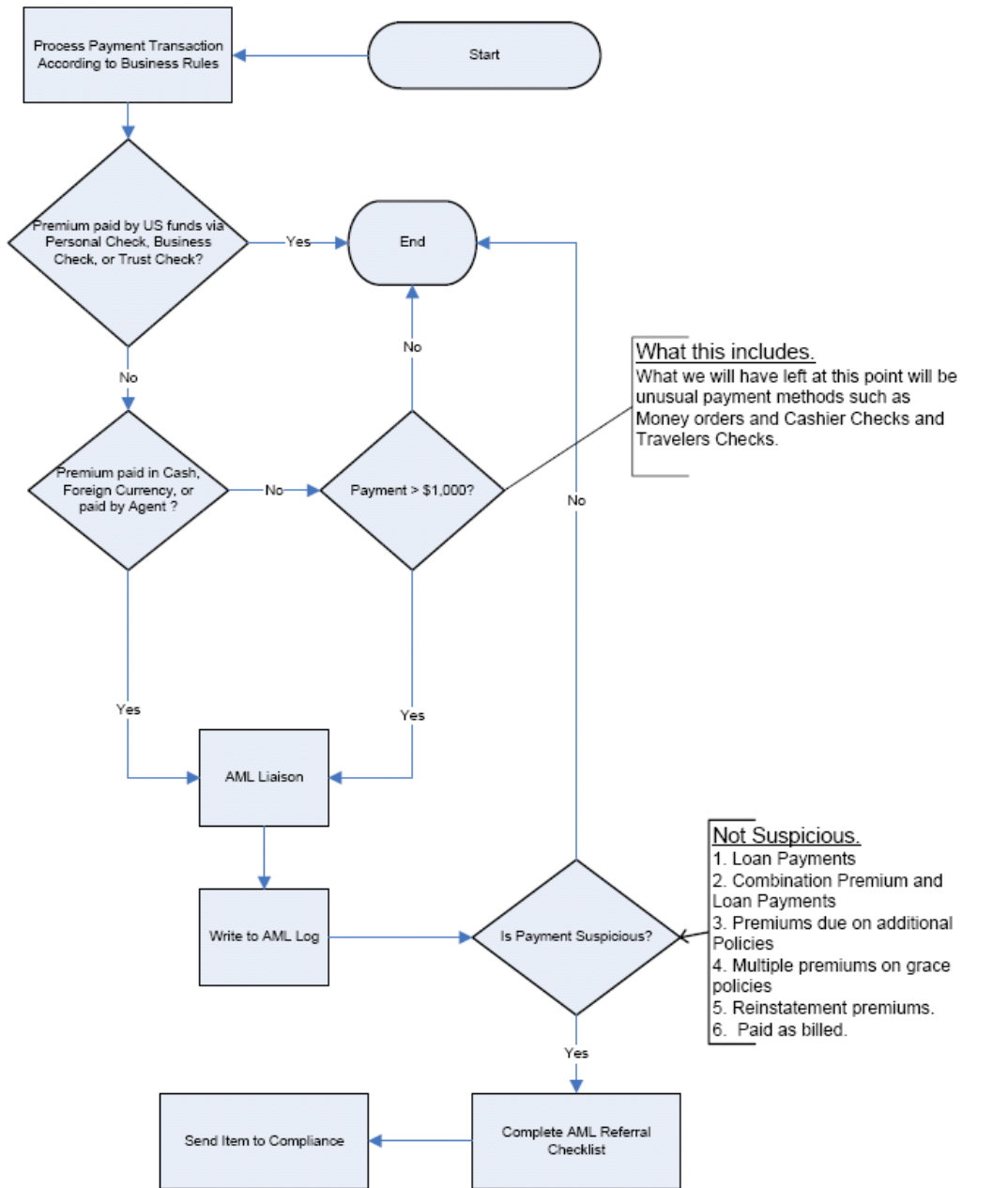
- Write to AML Log
- Complete AML Referral Checklist
- Send item to Compliance

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

## Wilmington Annuity Refund of Premium within Free Look Period



# Wilmington Annuity AML – Lockbox Exception Payments & Non-Lockbox Premium Procedures



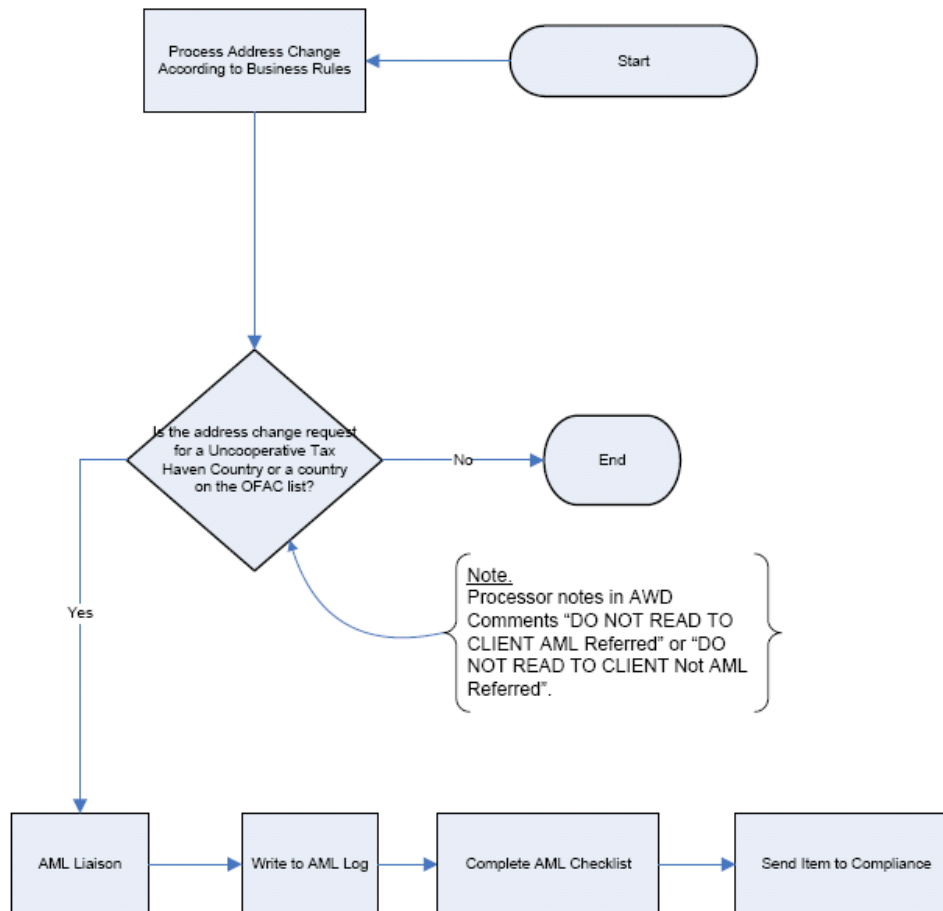
Wilmington Annuity AML Procedures.vsd Friday, August 25, 2006

version 1.0

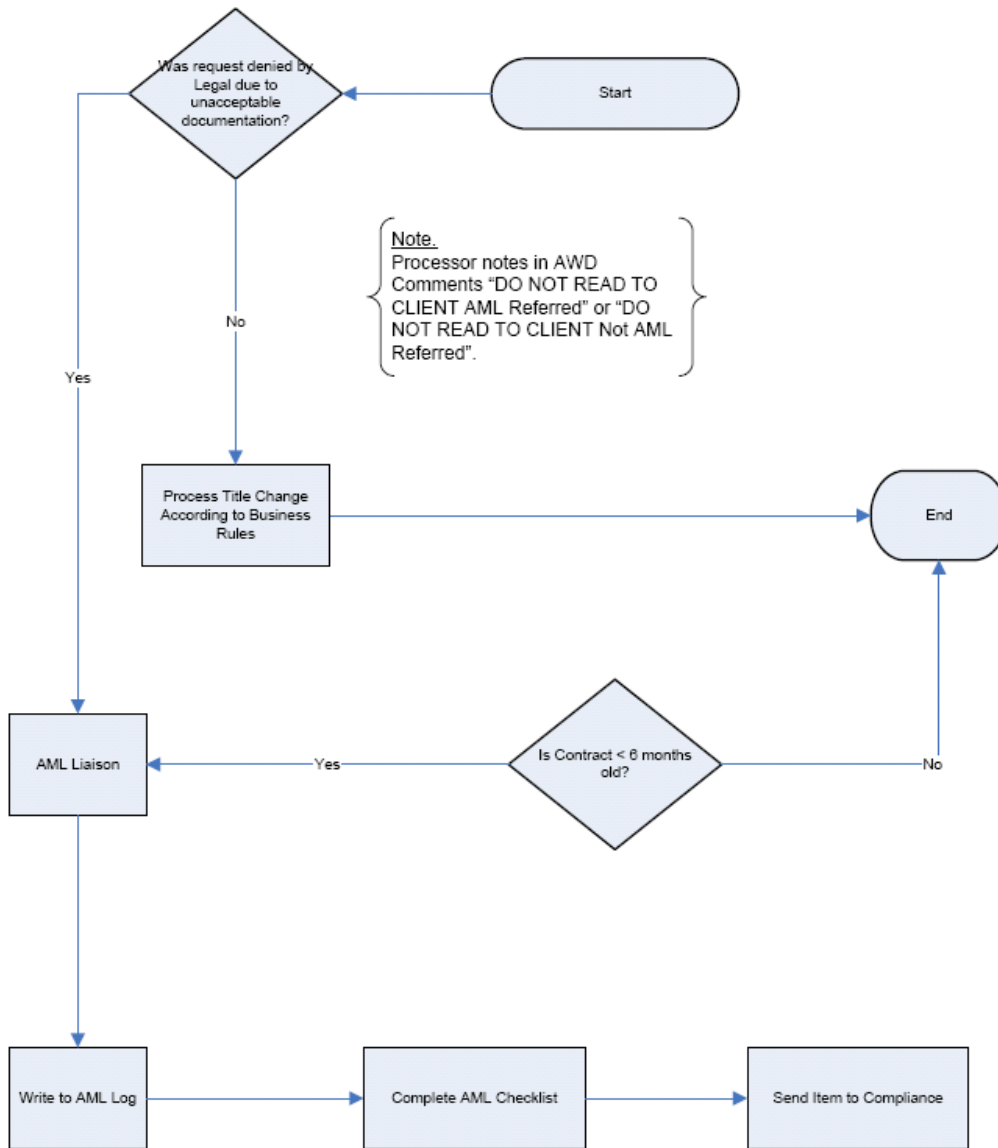


---

## Wilmington Annuity AML - Address Change Procedures



## Wilmington Annuity AML - Owner & Beneficiary Changes





**WILMINGTON ANNUITY ADMINISTRATION  
ANTI-MONEY LAUNDERING (AML)  
REFERRAL CHECKLIST**

This cover page should be used when referring an AML case to Compliance for review. Be sure this entry is also added to the Anti-Money Laundering Activity Log.

DATE REFERRED: \_\_\_\_\_ REFERRED BY: \_\_\_\_\_

SITE/DEPARTMENT: \_\_\_\_\_

Place checkmark in box for AML Activity being reported.

New Business Activity	Premium & Unusual Payment Activity	POS Activity
New Business Initial Premium	Exception Payments	Beneficiary Change
Refund of Premium Within Free Look Period		Ownership Change
Red Flag - Initial Review		Address Change
Red Flag – Underwriter Review		

System Affected: \_\_\_\_\_

Contract Number: \_\_\_\_\_

Client Name: \_\_\_\_\_

Brief description of AML activity being reported (attach any supporting documentation):

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

For Compliance Use Only:  
Assigned to: \_\_\_\_\_  
SAR submitted \_\_\_\_\_

Date: \_\_\_\_\_  
No SAR required \_\_\_\_\_

---

## **AGLA Policyowner Services**

Based on the risk assessment, the following procedures are to be followed to monitor transactions for suspicious activity:

### **Title Change**

#### *Owner & Beneficiary Change*

- Was request denied due to unacceptable documentation?
  - Yes
    - Refer to AML Liaison
  - No
    - Process Title Change according to Business Rules
    - Is product Term, A&H, Disability Income, or Group?
      - Yes – Process – no further action required
      - No
        - Is Face > \$100,000 & Policy inforce < 6 months?
          - Yes – refer to AML Liaison
          - No – process according to Business Rules

#### *Address Change*

- Process address change according to Business Rules
  - Is product Term, A&H, Disability Income, or Group?
    - Yes - Process – no further action required
    - No
      - Is the address change to a foreign country?
        - Yes – refer to AML Liaison
        - No – process according to Business Rules

### **Disbursements**

#### *Not Taken Offer (NTO)*

- Process NTO according to Business Rules
  - Is product Term, A&H, Disability Income, or Group?
    - Yes – Process – no further action required
    - No - Is NTO > \$5,000
      - No – Process – no further action required
      - Yes - Is NTO payment being refunded made within the last 3 months?
        - Yes – refer to AML Liaison
        - No – Process – no further action required.

---

### *Surrender, Partial, & Prepay Withdrawal*

- Process Disbursement according to Business Rules
  - Is Disbursement > \$5,000 & policy has been in force < 1 year?
    - No – Process – no further action required
    - Yes – Is Disbursement a 1035 Exchange or Rollover?
      - Yes – Process – no further action required
      - No – Premium/Prepay Dump-In > \$5,000 in last 3 months?
        - Yes – refer to AML Liaison
        - No – Is Surrender Charge > 25% of cash value?
          - Yes – refer to AML Liaison
          - No – Is Disbursement being sent to a foreign country?
            - Yes – refer to AML Liaison
            - No – Process – no further action required

### *Loan*

- Process Loan according to Business Rules
  - Is Loan > \$5,000?
    - No – Process – no further action required
    - Yes – Any evidence of Premium Dump-In in last 3 months?
      - Yes – refer to AML Liaison
      - No – Have there been multiple Loans & Loan Payments in the past year?
        - Yes – refer to AML Liaison
        - No – Has a Collateral Assignment been made in the last 3 months?
          - Yes – refer to AML Liaison
          - No – Is Loan being sent to a foreign country?
            - Yes – refer to AML Liaison
            - No – Process – no further action required

---

### *Premium Refund*

- Process Refund Transaction according to Business Rules
- Is product Term, A&H, Disability Income, or Group?
  - Yes – Process – no further action required
  - No – Is Refund > \$5,000?
    - No – Process – no further action required
    - Yes – Was payment being refunded made within the last 3 months?
      - Yes – refer to AML Liaison
      - No – Is Refund check being sent to a foreign country?
        - Yes – refer to AML Liaison
        - No – Process – no further action required

---

### **AML Liaison**

AML Liaison should do the following with items referred to them:

- Write to AML Log
- Complete AML Referral Checklist
- Send item to Compliance

**REFER TO GENERAL INFORMATION SECTION FOR LISTING OF TAX HAVEN COUNTRIES, OFAC BLOCKED COUNTRIES AND SUSPICIOUS ACTIVITY RED FLAGS FOR YOUR BUSINESS AREA.**

---

## AGLA Cash Payment Procedures

In the event that a customer includes any cash or coins in their payments, the processor opening the payment must immediately place it back in the envelope along with any other items i.e. check, money order, payment coupon, etc.

The employee then writes the words "Cash Payment" on the envelope, keeps the envelope in their possession, and calls either the Payment Processing Supervisor or the Reconciliation Analyst to advise them that they have received a cash payment.

The Payment Processing Supervisor or the Reconciliation Analyst enters the Processing Room and removes the envelope and its contents from the processor and log the contents into the Cash Payment Log located in the payment processing room. The employee specifically notates the date the cash was received in the payment processing room, the amount of the cash, the amount of the checks or money orders, the employee who received the cash, and the employee who logs the entry and locks up the envelope and its contents.

The Payment Processing Supervisor and the Reconciliation Analyst are the only two individuals who have keys to the locked cash box. One of them will then take the envelope and its contents and place them in the locked cash box.

The Cash Payment Log is checked daily, by the Reconciliation Analyst, to determine if there have been any cash payments. If there has been a cash payment, the Reconciliation Analyst proceeds to remove all of the payment coupons and checks or money orders from the locked cash box; however, all cash remains in the locked cash box. Notation is then made regarding the amount of the checks and or money orders and the amount of cash on each payment coupon.

The Reconciliation Analyst adds the total of all of the transactions (checks, money orders, and cash) on a receipt tape and applies the money using CPPS batch as requested and prints the copy of the CPPS batch. A copy of the receipt tape is attached to the CPPS batch.

The Reconciliation Analyst adds all cash and creates two receipt tapes and then adds all checks and money orders and creates two receipt tapes. Notation is then made of the CPPS batch, account number 146112, and "Cash" on the bottom of each receipt made for the cash. The same process is completed for checks and/or money orders.

The Reconciliation Analyst uses the total of all of the transactions to prepare a cash receipt voucher (CA) and debits account number 020001 (Cash Prem) and credits account number 146112 to offset the CPPS batch. The CA is printed three times.

Cash is then removed from the locked cash box, by the Reconciliation Analyst, and placed with the CA copy and receipt tapes. The Reconciliation Analyst signs the Cash Payment Log indicating that they have removed the money and notates the CA number to show where the money was submitted to the company.

One copy of the CA is submitted to the other Reconciliation Analyst along with one of the receipt tapes for the checks, one receipt tape for the cash, and a copy of the CPPS batch.

One copy of the CA with the checks and the receipt tape is taken to the Treasury cash counter and signed in.

One copy of the CA with the cash and the receipt tape is then taken to the Treasury cash counter and signed in notating the employee's name, the total cash amount, and the CA number.



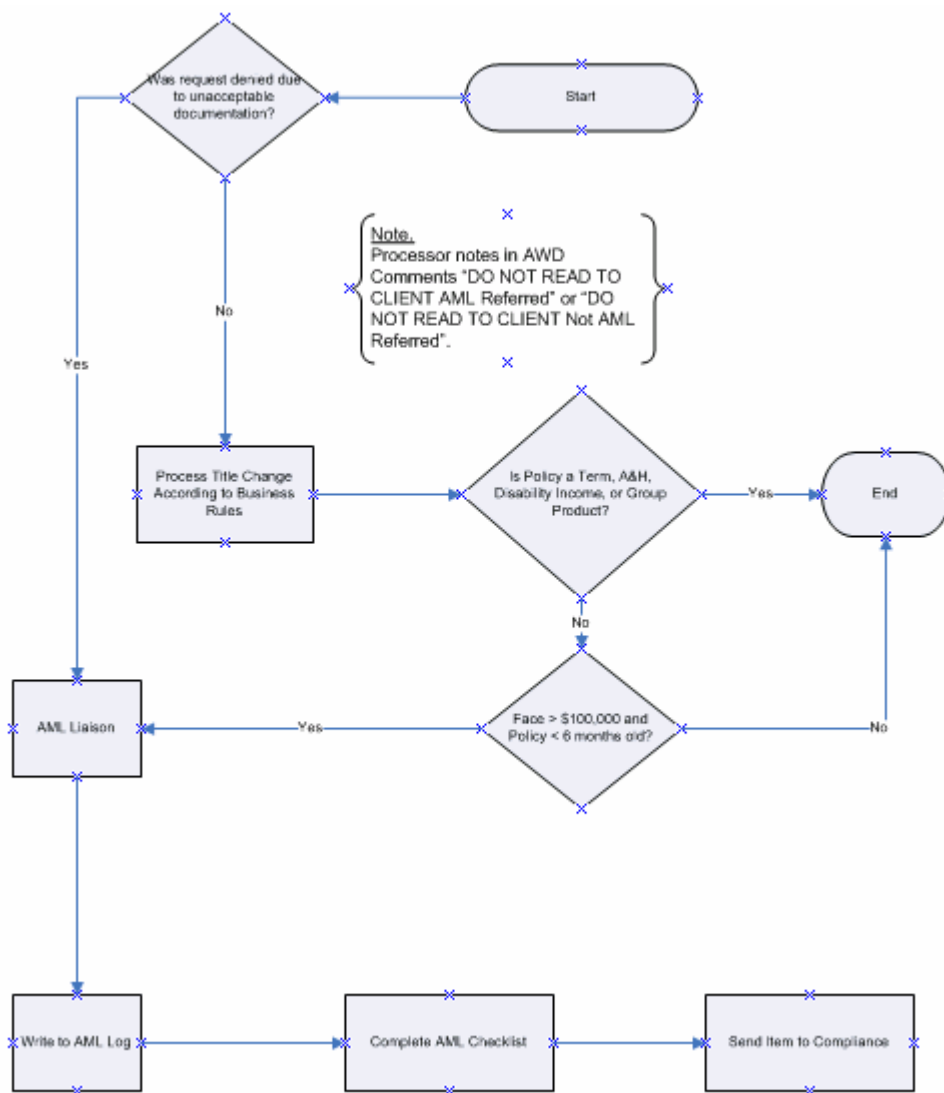
---

## **AGLA Monthly Compliance Procedures**

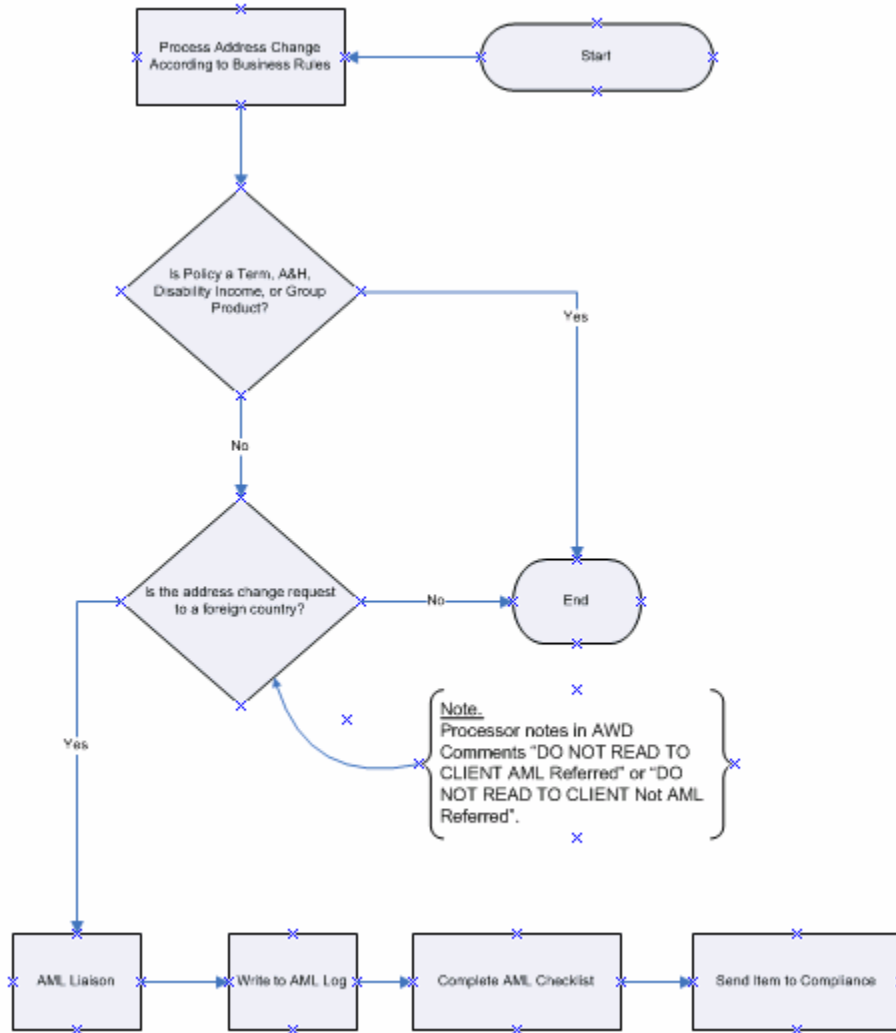
- Matching of agent's daily closeout reports including tests to ensure that notations of checks vs. cash are accurate. A monthly sample of 10% of closeouts in the amount of \$10,000, or greater, is conducted to assure proper notations of checks vs. cash.
- Monthly review of all suspicious transactions that have been referred to the respective business area's management. This procedure provides written documentation of why certain possible SAR transactions were not referred or why a SAR was not prepared.
- Monthly review of Cash Received Log to identify possible suspicious activity.



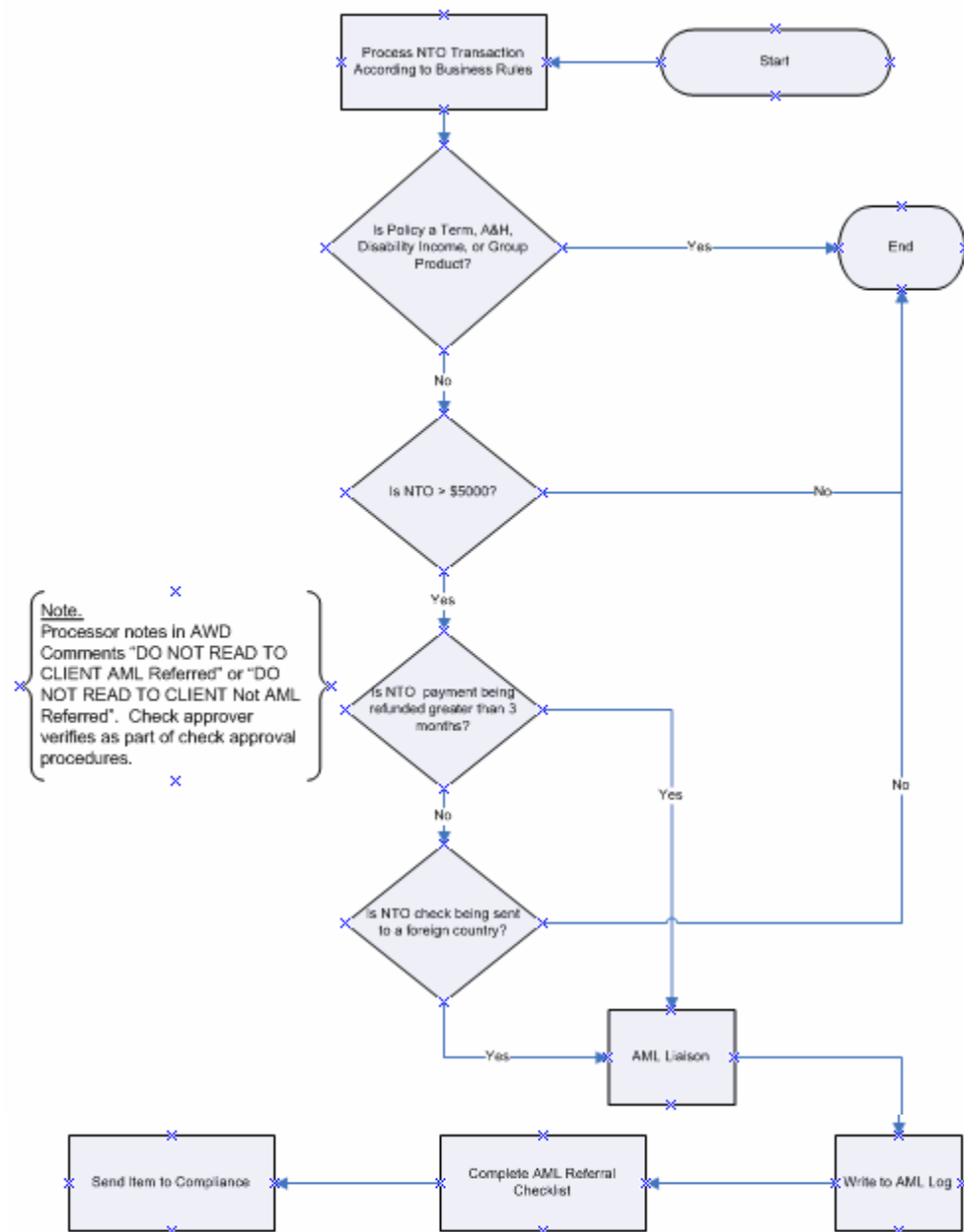
# Owner & Beneficiary Changes



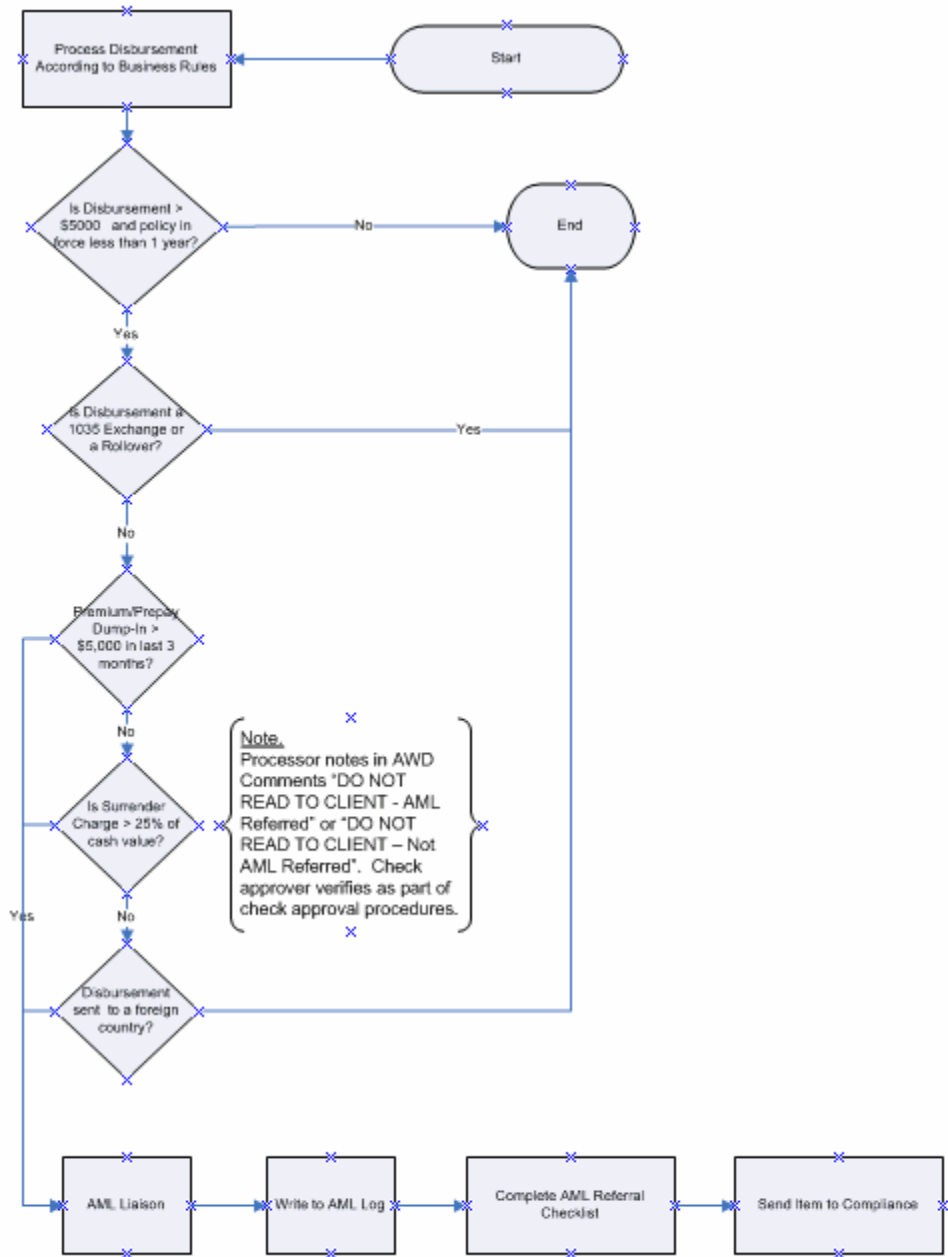
# AML – Address Change Procedures



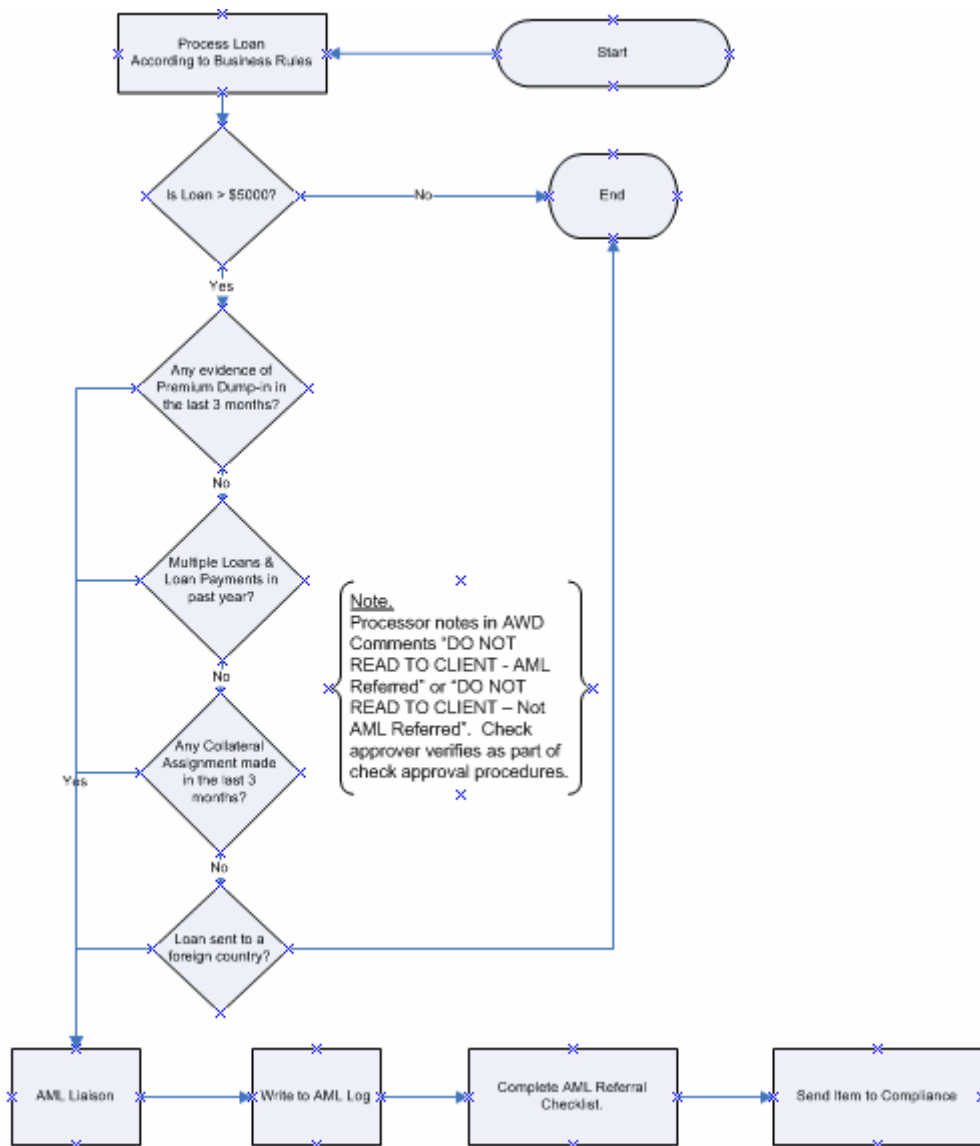
# AML – NTO Procedures



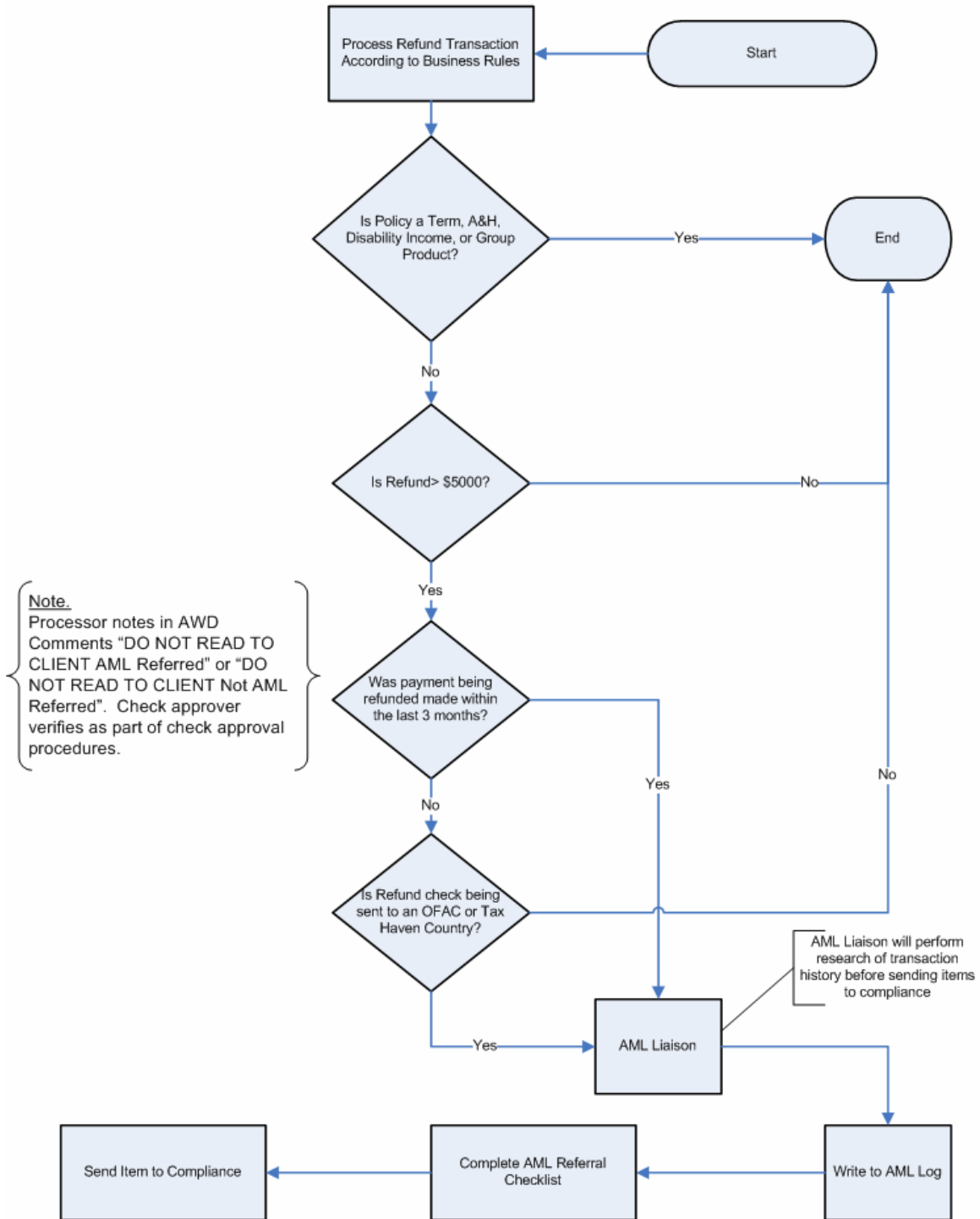
# AML – Disbursement – Surrenders, Partial and Prepay W/D Procedures



# AML – Disbursement – Loan Procedures



## AML – Premium Refund Procedures







## ANTI-MONEY LAUNDERING (AML) REFERRAL CHECKLIST

This cover page should be used when referring an AML case to Compliance for review. Be sure this entry is also added to the Anti-Money Laundering Activity Log.

DATE REFERRED: \_\_\_\_\_ REFERRED BY: \_\_\_\_\_

SITE/DEPARTMENT: \_\_\_\_\_

Place checkmark in box for AML Activity being reported.

New Business Activity	Premium & Unusual Payment Activity	POS Activity
Refund Check	Unusual Payment Method	Beneficiary Change
Red Flag – Underwriter Review	Exception Processing	Ownership Change
	History/Pattern Review	Address Change
		Surrender – Full or Partial Loan

System Affected: \_\_\_\_\_

Policy Number: \_\_\_\_\_

Client Name: \_\_\_\_\_

Brief description of AML activity being reported (attach any supporting documentation):

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Has AWD been noted about AML referral? \_\_\_\_\_

For Compliance Use Only:

Assigned to: \_\_\_\_\_

SAR submitted \_\_\_\_\_

Date: \_\_\_\_\_

No SAR required \_\_\_\_\_

---

## Treasury

Houston Treasury receives live checks from the Scan Center, along with a cover sheet identifying the item(s) as an AML exception. The Scan Center forwards a copy of the item to the appropriate admin area for research. The admin areas notify Treasury as to the disposition of the item – either deposit or return to sender. The admin areas are responsible for notifying Compliance of these items.

Houston Treasury also receives check copies for lockbox exception items from Citibank. Money orders are noted and suspended to the appropriate admin area separately so they can be researched for AML purposes, if necessary.

## High Dollar Disbursement Review

- Disbursement request for \$50,000 or greater are presented to Treasury with a High Dollar Disbursement Review Supporting Documentation Checklist which includes the following AML review items:
  - Review Large Premium Overpayments followed by Premium Refund Request
  - Review Large Dollar Deposits followed by High-Dollar Loan Request
  - Review wire transfers to high-risk countries or off-shore banks

**AIG American General  
High Dollar Disbursement Review  
Supporting Documentation Checklist**

Contract Owner \_\_\_\_\_  
Policy Number \_\_\_\_\_

PROVIDED

**CLAIM PAYMENT**

Policy Application	<input type="checkbox"/>
Policy Value (Status)	<input type="checkbox"/>
Claimant Statement	<input type="checkbox"/>
Death Certificate	<input type="checkbox"/>
Change of Beneficiary Form	<input type="checkbox"/>
Letters Testamentary	<input type="checkbox"/>

**SURRENDERS/LOANS**

Policy Application	<input type="checkbox"/>
Policy Value (Status)	<input type="checkbox"/>
Surrender Request	<input type="checkbox"/>
Signature Verification	<input type="checkbox"/>
1035 Exchange only	Letter of Acceptance <input type="checkbox"/>
	Change of Ownership Form <input type="checkbox"/>
	Trust Affidavit Form <input type="checkbox"/>
	Variable Policy (Transaction Date) <input type="checkbox"/>

		<b>Yes</b>
<b>Approval:</b>	Has disbursement been approved in accordance with company business policy?	<input type="checkbox"/>
<b>Mailing Address:</b>	Is check being delivered to address of record?	<input type="checkbox"/>
<b>Audit Letter:</b>	Is audit letter or disbursement confirmation needed?	<input type="checkbox"/>
<b>Reissue:</b>	If check is a reissue - has cancellation/stop been verified?	<input type="checkbox"/>
<b>Anti-Money Laundering Review</b>	Review Large Premium Overpayments followed by Premium Refund Request.	<input type="checkbox"/>
	Review Large Dollar Deposits followed by High-Dollar Loan Request.	<input type="checkbox"/>
	Review wire transfers to high-risk countries or off-shore banks.	<input type="checkbox"/>

Comments \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Reviewer Initials \_\_\_\_\_

Date \_\_\_\_\_

---

## **Licensing & Commissions**

### ***Notification of training requirement***

#### **Existing Agent**

- Initial bulletin published December 2005
- AML Introduction & Red Flag Bulletin – May 2, 2006
- Roll-out bulletin publication – July 11, 2006
- Follow-up “Reminder” bulletin(s) publication as needed

#### **New Agent Appointment**

- Information regarding training requirement, training site, logon detail and Welcome to the Company, included in Agent Appointment Application
- Follow-up “Reminder” bulletin(s) publication as needed

### ***Roll-Out Training program***

#### **LIMRA web-based AML program**

- obtain training through secure website or Brainshark
- LIMRA notifies Company of training completion

#### **AML training other than LIMRA**

- Agent notifies Company that his AML training was completed through another source and provides specific documentation
- External training is validated by Compliance

### ***Follow-up for agent non-compliance***

#### **Pending Application Process**

- If New Business receives an application for an agent who has NOT completed the required AML Training, NB notifies L&C.
- L&C contacts the agent, who is given 5 days to complete the training or provide certification that training was previously completed.
- If training is not completed within the specified time frame, NB is notified to return the application to the agent.

---

# Training

## ***Initial Training***

Initial AML training is provided online. The training program is web-based and currently has the following 4 modules of specialized training:

- Broker / Dealer – Securities related
- Agent – specifically addresses “Red Flag” scenarios a producer might witness
- Office Employee – specifically addresses “Red Flag” scenarios an office employee might encounter during normal transaction processing
- Canadian Agent – Specific to Canadian AML rules – Not Applicable to American General Domestic Life Operations

American General is provided reports with information about who has or has not completed the training. Licensing & Commissions will follow the “Pending App” protocol for non-compliant producers who submit an application. Human Resources will follow established protocol for non-compliant employees.

## ***Ongoing AML Training***

Domestic Life Compliance has also developed an AML Refresher Training schedule. This involves regular email communications targeting specific business units which highlight various AML topics (AML Facts, Red Flags, etc). There are also bulletins sent to all Domestic Life Compliance employees, which cover general AML information, crossword puzzles using AML terminology and general Red Flag scenarios. Each communication includes a link to the Compliance website.

## Global Watch List

The OFAC/CIP team reviews the following Global Watch List for hits:

Entity Source Code	Full Name of List (or Source)	OFAC records – Type of data
11	US Treasury Specially Designated Nationals List (OFAC)	OFAC's SDN list
33	Government Officials (OFAC)	Government officials of sanctioned countries obtained from the CIA's Chief of State and Cabinet members of Foreign Governments
44	Restricted for Blocked Locations (OFAC)	Geographical. (principal cities in embargoed countries, states, provinces, alternate/local spellings)
22	Accuity Research (OFAC)	Entries of sanctioned governments, alternate spellings of sanctioned entities, and transactions
77	Accuity's World Bank Directory (OFSC)	Additional locations and data for banks affected by sanction programs, including SWIFT/BIC addresses
88	U. S. State Department (OFAC)	Principal members of Foreign Terrorist Organizations

### ***OFAC Team Procedures***

#### **Daily Check, Payrte & New Business runs & Weekly In force runs**

When Entity Source Codes (see above chart) are received and the hit matches the client/payee name or country, it is validated by the OFAC team using various resources such as Lexis Nexis, CCIV, AWD and applicable mainframe systems. If necessary, other Company service center locations (Nashville, Dallas, Springfield, Milwaukee, or Amarillo) will be contacted for additional information.

## AML Compliance Committee

---

The Anti-Money Laundering Compliance Committee shall be responsible for making and enforcing the Company's Anti-Money Laundering Policy and Procedures.

Membership. The Company shall have an Anti-Money Laundering Compliance Committee (AMLCC). The current membership is:

AML Compliance Officer, Chairperson  
General Counsel  
General Auditor

The Committee may designate any other individuals for specific committee meetings or portions of committee meetings as they deem appropriate.

Responsibilities. The AMLCC has the following responsibilities:

- Review, at least annually, the existing Company anti-money laundering compliance policy and procedures, and to recommend changes, if necessary.
- Ensure that appropriate training and education is provided to Company employees, agents, and representatives regarding the Company's anti-money laundering policy and procedures.
- Ensure that an effective audit program is established and maintained with regard to the Company's anti-money laundering policy and procedures.
- Review allegations, any related investigations, and other evidence of violations of policies and procedures by any Company employee, agent, or representative.



## **Reporting Suspicious Activity**

---

Suspicious transactions should be referred to a member of the respective business area's management. If the business area management agrees that a particular transaction, or aggregate of transactions, warrants additional review, the item(s), and supporting documentation, should be referred immediately to the Compliance Department, where additional due diligence will take place. Upon thorough review by the Compliance Department, transactions that appear to be suspicious will be referred immediately to the Company's AML Compliance Officer and/or the Anti-Money Laundering Compliance Committee.

The AML Compliance Officer for the Company will perform the necessary compliance functions relating to the Company's Anti-Money Laundering Policy and procedures. The AML Compliance Officer shall, when deemed appropriate, be responsible for submission of Suspicious Activity Reports (SAR – Appendix C) with the Financial Crimes Enforcement Network of the US Department of the Treasury.

# APPENDIX A

## ***Business Policy 0315***

**BUSINESS POLICY FOR AIG AMERICAN  
GENERAL**



Subject: 0315 Global Money Laundering Prevention Policy

Policy Number: 0315

Revision B

Code:

### **CORPORATE POLICY & PROCEDURES:**

The Corporate policy against money laundering is available at <http://livpwsb13.aig.com/cfcompliance/AIG%20Interim%20Anti-Money%20Laundering%20Policy.pdf>. It includes:

- Background
- Key concepts
  - Money laundering
  - Terrorist financing
- Basic program requirements
  - Client identification and verification
  - Due diligence and enhanced due diligence
  - Transaction monitoring
  - Reporting
  - Terminating a relationship
  - Government requests for information
- Record-keeping
- Monitoring and auditing
- Training
- Business unit role and penalties

**QUESTIONS** may be referred to your business unit chief compliance officer.

### **DOMESTIC LIFE COMPANIES POLICY & PROCEDURES:**

**PURPOSE.** The purpose of this business policy is to set forth policies and procedures designed to:

- Comply with the anti-money-laundering rules for insurance companies;
- Comply with the Bank Secrecy Act; and
- Prevent or detect illegal activity and rule violations pertaining to money laundering, and facilitate a quick, effective response to such activity.

**EFFECTIVE.** This policy has been in effect since May 2, 2006.

## DEFINITIONS.

**Money Laundering.** Money laundering is defined under federal law to mean the movement of illicit cash or cash equivalent proceeds into, out of, or through the United States or its financial institutions.

**Financial Institution.** The term "financial institution" includes insurance companies.

**Illicit.** "Illicit" encompasses virtually any federal or state felony as well as numerous crimes such as wire, mail, and securities fraud.

## BACKGROUND.

**Patriot Act.** In 2001 the president signed into law the USA Patriot Act (International Money Laundering Abatement and Anti-terrorist Financing Act of 2001) that requires financial institutions, including insurance companies, to establish and implement compliance programs regarding money laundering. These programs should be designed to ensure ongoing compliance with the requirements of the Bank Secrecy Act and the regulations promulgated thereunder.

**Agency Rule.** The Department of the Treasury delegated to the Director of the Financial Crimes Enforcement Network (the "Agency") the creation and implementation of the applicable rule (the "Rule") for insurance companies. The Agency issued the Rule effective December 5, 2005, which requires an insurance company offering covered products (as defined by the Rule) to develop and implement by May 2, 2006, a written anti-money-laundering program applicable to its covered products. For purposes of the Rule, covered products include a permanent life insurance policy (other than a group life insurance policy), an annuity contract (other than a group annuity), and any other insurance product with features of cash value or investment. The program must be reasonably designed to prevent the insurer's facilitation of money laundering or the financing of terrorist activities. The program must also be made available to specified regulatory agencies upon request.

**Penalties.** There can be severe criminal penalties for violations of the federal money laundering provisions, including substantial fines and lengthy prison terms. Under the Money Laundering Control Act of 1986, financial institutions may be prosecuted for assisting or participating in money laundering activities conducted by their customers.

## GUIDELINES, RESPONSIBILITIES, AND PROCEDURES.

**General Anti-money-laundering Guidelines.** Listed below are actions that are fundamental to the AIG American General Companies' policy and procedures to prevent money laundering. AIG American General employees, agents, or representatives engaging in these activities are subject to disciplinary action, including termination, for violation of these guidelines.

**Transactions.** No AIG American General employee, agent, or representative shall:

- Be involved in, or assist with what he/she knows, or should have known, to be money laundering activity or transaction; or
- Consider doing a financial transaction if he/she knows, or should have known, that the transaction is furthering a crime or that the funds are from illegal sources.

**Customer Knowledge.** All AIG American General agents, employees, and representatives shall take reasonable steps to know their customers, with a view toward preventing and avoiding money laundering.

**Supervision.** All AIG American General home office managers will take all reasonable steps to supervise their employees, agents, and representatives with a view toward preventing and avoiding money laundering.

**Anti-money-laundering Compliance Committee.** The anti-money-laundering compliance committee shall be responsible for making and enforcing AIG American General's anti-money-laundering policy and procedures.

**Membership.** AIG American General shall have an Anti-money-laundering Compliance Committee. The current membership is:

Deanna D. Osmonson, Compliance Officer and Anti-money-laundering Compliance Officer, AIG American General, Chair  
Kyle Jennings, General Counsel, Litigation and Compliance, AIG American General  
George Jovanovic, Anti-money-laundering Compliance Officer, AIG Life Insurance Company of Canada  
John Kancans, Anti-money-laundering Compliance Officer, American International Group  
Dale Stewart, Vice President and General Auditor, AIG American General

The Committee may designate any other individuals for specific committee meetings or portions of committee meetings as they deem appropriate.

**Responsibilities.** The Anti-money-laundering Compliance Committee has the following responsibilities:

**Policies and Procedures.** Review, at least annually, the existing AIG American General anti-money-laundering compliance policy and procedures and recommend changes, if necessary.

**Training and Education.** Ensure that appropriate training and education is provided to AIG American General employees, agents, and representatives regarding the anti-money-laundering policy and procedures.

**Audit Program.** Ensure that an effective audit program is established and maintained with regard to AIG American General's anti-money-laundering policy and procedures.

**Evidence of Violations.** Review allegations, any related investigations, and other evidence of violations of policies and procedures by any AIG American General employee, agent, or representative.

**Procedures Regarding Opening an Account or Selling a Life Insurance Policy or Annuity Contract.** In addition to the information required on the application or new account form, AIG American General employees, agents, and representatives must be alert to other risk factors that may appear. If an AIG American General employee, agent, or representative has a reason to believe that a risk factor is present, he/she must promptly notify their profit center compliance officer. The profit center compliance officer, in conjunction with the Anti-money-laundering Compliance Committee, will begin an analysis of the account proposed to be opened or the policy or contract proposed to be sold. The AIG American General Anti-money-laundering Compliance Committee or its designee(s) will conduct a review of all the factors identified that are presented by the proposed new account and/or purchase and will determine from that review the standard of due diligence

to be used in determining whether the account may be opened and/or the sale may be completed.

**Withdrawals, Surrenders, and Liquidations.** AIG American General Companies' employees must also be alert for [risk factors](#) that might appear when an individual attempts a withdrawal from or the surrender of a life insurance policy or annuity contract or to otherwise liquidate a holding. If an AIG American General employee has a reason to believe that a risk factor is present in a withdrawal, surrender, or liquidation situation, he/she must promptly notify their profit center compliance officer. The profit center compliance officer, in conjunction with the Anti-money-laundering Compliance Committee, will begin an analysis of the proposed distribution of funds. The Anti-money-laundering Compliance Committee or its designee(s) will conduct a review of all the factors identified that are presented by the transaction and determine from that review the standard of due diligence to be used in determining whether to allow the withdrawal, surrender, or liquidation.

**Responsibilities When Opening an Account or Taking an Application for a Life Insurance Policy or Annuity Contract.** In addition to all other requirements for opening an account and/or taking an application for a life insurance policy or an annuity contract, AIG American General agents and representatives shall take reasonable steps to verify the identity of all customers and the nature of a customer's transaction. These steps may include, but are not limited to, obtaining:

- Satisfactory identification to corroborate the client's identity (e.g., driver's license with photo and US passport);
- Basic background information on a customer such as residence and place of business; or
- Information on a client's source of funds/wealth to fund the transaction or open account.

**Compliance Activity.** The Chief Compliance Officer, AIG American General, will perform the necessary compliance functions relating to AIG American General's anti-money-laundering policy and procedures. The Chief Compliance Officer shall, when deemed appropriate, be responsible for submission of Suspicious Activity Reports to the Agency.

**OFAC.** AIG American General is subject to the provisions of the various sanctions and programs administered by the Office of Foreign Asset Controls (OFAC). These include prohibitions against trading with certain identified enemies of the United States as set forth in various lists prepared by OFAC and other governmental agencies.

**QUESTIONS** may be referred to Deanna D. Osmonson, Compliance Officer, AIG American General.

**DOMESTIC LIFE COMPANIES BUSINESS POLICY ADMINISTRATION:**

Category: 0300s: Legal Group: 0300s: Legal

Release Date: 04/28/2008 Next Review Date: 03/28/2009

Revised to update the membership of the anti-money laundering compliance committee.

Source: January 15, 2009, e'mail from Suzanne Rich Folsom, Chief Regulatory & Compliance Officer/Deputy General Counsel, AIG

December 2008

## **Interim Global Anti-Money Laundering Policy**

### **Background**

It is AIG's policy to not have its products or services used or abused for money laundering or financing terrorism purposes.

AIG's Global Anti-Money Laundering Policy establishes principles and global minimum standards to protect AIG from being used to launder funds or finance terrorism. AIG is bound by the Anti-Money Laundering (AML) laws and Counter Terrorist Financing (CTF) laws in its operating jurisdictions. This policy's minimum standards apply to all AIG Business Units and require them to implement AML and CTF policies required by law. This policy is effective December 2008.

AIG Business Units and Corporate Compliance Officers (CCOs) are required to establish antimoney laundering and counter terrorist financing programs consistent with this interim policy, applicable laws, and/or on a risk-based basis. The Global Regulatory and Compliance Group will work with designated Business Units CCOs to establish and implement oversight of this policy and related procedures and controls on a local basis. Each AIG Business Unit is responsible for ensuring that monitoring processes designed to detect and prevent violations of this policy are implemented.

Money Laundering is regulated by many U.S. and non-U.S. laws, including, but not limited to:

- The USA's Bank Secrecy Act, as amended by the USA Patriot Act;
- The UK's Money Laundering Regulations 2007 and Proceeds of Crime Act;
- Canada's Proceeds of Crime (Money Laundering) and Terrorism Financing Act;
- Australia's Anti-Money Laundering and Counter Terrorism Act Financing Act of 2006;
- India's Prevention of Money Laundering Act; and
- China's Bill of Anti-Money Laundering

These laws have common themes requiring AML programs to have policies, procedures and controls, compliance staff, training, client identification verification, monitoring of client activity, reporting suspicious or unusual activity to governments and/or regulatory authorities, sharing information with such authorities upon request, and independent testing. However, each has distinct specifications which require AIG Business Unit CCOs to review them in detail and determine the nature and extent of the process and procedures.

### **Key Concepts**

- **Money Laundering** – Occurs when criminally derived funds or assets, including cash and securities, are moved through the global financial system to disguise their unlawful origin and/or true ownership. It can be committed through knowingly engaging in an illegal financial transaction or by deliberately ignoring indications of suspicious activity regarding a client or transaction.
- **Terrorist Financing** – The financial support of terrorist acts and those who commit them. Terrorist financiers seek to transfer funds in a way that conceals their source and intended use.

December 2008

### **Basic Program Requirements**

Based on an appropriate risk assessment by each Business Unit of its products, services and customers, each Business Unit must establish appropriate policies, procedures and controls covering (where applicable) the following areas:

- **Client Identification and Verification** – AIG Business Units must comply with applicable client identification and verification laws and regulations, and implement client identification programs using a risk-based approach.

- **Due Diligence and Enhanced Due Diligence** – AIG Business Units must exercise sound judgment when evaluating agent, broker, employee, service provider, client or counterparty relationships and satisfy themselves that such parties do not present undue legal, regulatory or reputational risk to AIG. When required by law and/or on a risk-based basis, AIG will conduct due diligence on such parties.
- **Transaction Monitoring** – AIG employees are required to understand and monitor client transactions to detect, deter, investigate, and report money laundering or other suspicious activity.
- **Reporting** – Client transactions and other activities identified as potentially suspicious must be investigated in order to determine whether to file a report with the appropriate authorities, such as, in the U.S., a Suspicious Activity Report. In addition, procedures must be put in place to ensure that any other legally required reports (such as currency transaction reports) are recorded, reported and filed in accordance with applicable law.
- **Terminating a Relationship** – Business Unit CCOs, in consultation with relevant business and legal staff, will decide whether to terminate a client relationship based on risk concerns. The decision to terminate a business relationship should be communicated to relevant business, legal and compliance staff.
- **Government Requests for Information** – AIG employees who receive a subpoena or other request for information should notify their Business Unit CCO immediately, not discuss the order with anyone other than their Business Unit CCO, and direct any law enforcement agency to the relevant legal counsel or Business Unit CCO. The Business Unit CCO should consult with legal and compliance staff regarding the appropriate handling of such requests.

#### **Recordkeeping**

- AIG Business Units are required to prepare and maintain any AML-related records and any other required government reports (such as reports concerning the sale of monetary instruments) and to work with Business Unit CCOs to ensure appropriate record keeping. These records should be kept for a minimum of five years.

#### **Monitoring and Auditing**

- AIG Business Units will monitor their operations to ensure compliance with established policies, procedures and internal controls. The Global Regulatory and Compliance Group will have oversight responsibility for the compliance monitoring function.
- AIG's Internal Audit Department will conduct audits of AIG's AML Program, including client transactions, suspicious activity monitoring and reporting, and compliance with AIG's AML and CTF policies and procedures. Audit reports will be integrated on an ongoing basis into AIG's policies, procedures and controls.
- AIG Business Units that accept cash payments must have monitoring procedures to ensure compliance with applicable large currency reporting requirements.

December 2008

#### **Training**

- Each Business Unit is responsible for ensuring that employees and agents are appropriately trained on AIG's AML and CTF policies and procedures.

#### **Business Unit Role and Penalties**

AIG will take appropriate action against any employee whose actions are found to violate this policy up to and including termination. Disciplinary action also may be taken against responsible employees who unreasonably fail to detect or report such violations, as well as those who retaliate against those employees who report potential violations. In addition, penalties may include criminal, civil and regulatory penalties for AIG and its employees individually, including imprisonment and fines.

Where a determination is made that a Suspicious Activity Report or a Currency Transaction Report does not need to be completed, there should be written documentation of that determination.

#### **Contact**

- Employees should contact their Business Unit CCOs with questions regarding this policy.

Category: Compliance

Date: 04/28/2008

Subject: Money Laundering Risk Factors

### **General Information**

- A customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- A customer appears to operate as an agent for an undisclosed principal, and is reluctant to provide information regarding that entity.
- A customer has difficulty describing the nature of their business.
- A customer lacks general knowledge of their industry.
- A customer, or a person publicly associated with a customer, has a questionable background including prior criminal convictions.
- A customer attempts to open an account with unusual or suspect identification or business documents.
- A customer provides non-verifiable reference(s) or is reluctant or refuses to provide financial information or information concerning financial relationships and business activities.
- A customer questions if conducting certain asset movements would prompt reporting to the federal government.
- A customer repeatedly requests exceptions to policies and procedures set up to deter money-laundering activity.
- A customer requests pre-arranged codes or passwords to facilitate the transfer of cash or securities in the account.

### **New Accounts Information**

- Cash purchases of an insurance policy or annuity contract and then early "cashing out" of the policy/contract using its "free look" period, or an early surrender of the policy/contract minus a penalty.
- For no apparent reason, a customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- A customer is from, or has accounts in, a country identified as a haven for money laundering.
- Transactions involving an offshore corporation formed in a bank secrecy haven whose name is similar to that of a large well-known U.S. corporation.
- An account or transaction is for a personal holding company or an offshore corporation in a known tax haven.
- A customer, or one of his/her immediate family members or close associates, is a senior foreign political official.



## Cashiering Information


- A customer attempts to deposit multiple cashier's checks, money orders, or traveler's checks totaling more than \$10,000.
- A customer exhibits an unusual lack of concern regarding risks, commissions, or other transaction costs, or offers to pay higher than normal fees for the movement of money to and from other accounts and financial institutions.
- A customer requests that funds and investments be transferred to third parties, unrelated to any commercial or fiduciary purpose, especially frequent or large wire transfers or journals to/from individuals/organizations with no apparent business relationship.
- A customer receives and delivers multiple wire transfers to move large amounts of money to or from a jurisdiction that appears on the G-7 Blacklist or is an offshore tax haven. (For the G-7 Blacklist, see FinCEN Advisories issued July 2000.)
- A group of customers makes large numbers of deposits into different accounts with frequent balance transfers to a single account.
- Transactions involving an offshore corporation formed in a bank secrecy haven whose name is similar to that of a large well-known U.S. corporation.
- A customer deposits multiple checks and immediately uses a debit card to withdraw the funds.
- A customer attempts to deposit Reg S stock(s) without properly identifying them as such and attempts to borrow against them.
- A customer attempts to deposit multiple bearer instruments that appear old, musty, or are in some form of decay.
- Frequent requests for approval to conduct large cash withdrawals from banks through the use of debit cards.
- The opening of an account for a customer who is more interested in writing checks and utilizing a debit card than in investing.
- Frequent or large wire transfer to/from individuals/organizations with no apparent business purpose.
- Large check deposits followed closely by the wiring out of funds.
- The receipt of federal funds with immediate journals to other accounts (first- or third-party).
- A customer account receives or delivers multiple wire transfers in amounts less than \$10,000.
- An account develops a pattern of journalizing funds and securities to other accounts.
- A large volume of wire transfer requests to offshore banks.
- A customer makes frequent and large deposits into the account with immediate disbursements via checks.
- A customer requests that checks delivered from an account be made payable to foreign exchange houses (e.g., Casa de Cambios).
- A customer attempts to use third-party or cash-like checks to complete a transaction in the account.
- A customer requests the disbursement of funds from an account versus uncleared funds.
- A customer makes frequent requests to make exceptions to company policy as it relates to the movement of funds or securities, or deposit procedures.

- The receipt or attempted receipt of stock certificates that do not clearly indicate the true owner.
- Journals of money and securities between accounts that have little or no securities transactions and whose sole purpose is the movement of money.
- A customer frequently requests wire transfers or check disbursements at the close of business or before a holiday.
- A customer frequently advises that wire transfers were sent in error and requests their immediate return or that the wire be forwarded to another account.
- A customer account shows a large deviation from its normal pattern (e.g., sudden movement of funds into and out of the account, sudden requests to deliver large wire transfers to third parties).
- An account or transaction is for a personal holding company or an offshore corporation in a known tax haven.
- A customer attempts to deposit multiple cashier's checks, money orders, or traveler's checks totaling more than \$10,000.
- A customer attempts to deposit foreign bank drafts in any denomination.
- A customer frequently requests exceptions to deposit cash-like second-party or third-party checks.
- A large volume of federal fund wires, checks, journals, or securities are received or delivered to/from an account within a given period of time with little or no trading activity.
- Account that consistently requests exceptions to deliver third-party wires from their account.
- Checks, federal funds, or securities delivered from an account are consistently sent to foreign names and addresses.
- Checks, federal funds, or securities delivered from an account are not consistent with the client's stated business.
- A receipt of certificates with the immediate request that they be delivered to another firm.
- A customer frequently requests that certificates be delivered to a third party or repeatedly requests third-party certificate disbursements from an account.
- The customer deposits or attempts to deposit large quantities of multiple deposits of penny stocks.
- The receipts, deliveries, and deposits are inconsistent with the client's usual account activity.

### **Trading Information**

- A customer exhibits an unusual lack of concern regarding risks, commissions, or other transaction costs, or offers to pay higher than normal fees for the movement of money to and from other accounts and financial institutions.
- The customer engages in transactional activity surpassing the customer's known income/net worth.
- An account or transaction is for a personal holding company or an offshore corporation in a known tax haven.

# APPENDIX B - SAR Form

<b>FinCEN Form 101</b>  <small>Effective May 2004</small>	<b>Suspicious Activity Report by the Securities and Futures Industries</b> Please type or print. Always complete entire report. Items marked with an asterisk * are considered critical. (See instructions.)	 <small>CMB No. 1506 - 0019</small>
1 Check the box if this report corrects a prior report (See instructions) <input type="checkbox"/>		
<b>Part I Subject Information</b> 2 Check box a <input type="checkbox"/> if multiple subjects    box b <input type="checkbox"/> subject information unavailable		
*3 Individual's last name or entity's full name		*4 First name
		*5 Middle Initial
*6 Also known as (AKA - individual), doing business as (DBA - entity)		*7 Occupation or type of business
*8 Address		*9 City
*10 State	*11 ZIP code	*12 Country code (if not U.S.) (See instructions)
		*13 E-mail address (if available)
*14 SSN/ITIN (individual), or EIN (entity)		*15 Account number(s) affected, if any. Indicate if closed.
		Acc't # _____ yes <input type="checkbox"/> Acc't # _____ yes <input type="checkbox"/>
		Acc't # _____ yes <input type="checkbox"/> Acc't # _____ yes <input type="checkbox"/>
		*16 Date of birth
		MM DD / YYYY
*17 Government issued identification (if available)		
a <input type="checkbox"/> Driver's license/state ID    b <input type="checkbox"/> Passport    c <input type="checkbox"/> Alien registration    d <input type="checkbox"/> Corporate/Partnership Resolution		
e <input type="checkbox"/> Other _____		
f ID number _____		g Issuing state or country (2 digit code) _____
*18 Phone number - work ( ) ( ) - - - - -		*19 Phone number - home ( ) ( ) - - - - -
*20 Is individual/business associated/affiliated with the reporting institution? (See instructions)		
a <input type="checkbox"/> Yes    b <input type="checkbox"/> No		
<b>Part II Suspicious Activity Information</b>		
*21 Date or date range of suspicious activity		*22 Total dollar amount involved in suspicious activity
From MM / DD / YYYY To MM / DD / YYYY		\$: _____ .00
*23 Instrument type (Check all that apply)		
a <input type="checkbox"/> Bonds/Notes    i <input type="checkbox"/> Commodity options    q <input type="checkbox"/> Commodity type _____ (Please identify) b <input type="checkbox"/> Cash or equiv.    j <input type="checkbox"/> Security futures products    r <input type="checkbox"/> Instrument description _____ c <input type="checkbox"/> Commercial paper    k <input type="checkbox"/> Stocks    s <input type="checkbox"/> Market where traded _____ (Enter appropriate three or four-letter code.) d <input type="checkbox"/> Commodity futures contract    l <input type="checkbox"/> Warrants    t <input type="checkbox"/> Other (Explain in Part VI) e <input type="checkbox"/> Money Market Mutual Fund    m <input type="checkbox"/> Other securities f <input type="checkbox"/> Mutual Fund    n <input type="checkbox"/> Other non-securities g <input type="checkbox"/> OTC Derivatives    o <input type="checkbox"/> Foreign currency futures/options h <input type="checkbox"/> Other derivatives    p <input type="checkbox"/> Foreign currencies		
*24 CUSIP* number _____		*25 CUSIP* number _____
*26 CUSIP* number _____		*27 CUSIP* number _____
*28 CUSIP* number _____		*29 CUSIP* number _____
*30 Type of suspicious activity:		
a <input type="checkbox"/> Bribery/gratuity    h <input type="checkbox"/> Identity theft    o <input type="checkbox"/> Significant wire or other transactions without economic purpose b <input type="checkbox"/> Check fraud    i <input type="checkbox"/> Insider trading    p <input type="checkbox"/> Suspicious documents or ID presented c <input type="checkbox"/> Computer intrusion    j <input type="checkbox"/> Mail fraud    q <input type="checkbox"/> Terrorist financing d <input type="checkbox"/> Credit/debit card fraud    k <input type="checkbox"/> Market manipulation    r <input type="checkbox"/> Wash or other fictitious trading e <input type="checkbox"/> Embezzlement/theft    l <input type="checkbox"/> Money laundering/Structuring    s <input type="checkbox"/> Wire fraud f <input type="checkbox"/> Commodity futures/options fraud    m <input type="checkbox"/> Prearranged or other non-competitive trading    t <input type="checkbox"/> Other (Describe in Part VI) g <input type="checkbox"/> Forgery    n <input type="checkbox"/> Securities fraud		

Catalog No. 35349U

Rev. 05/22/04



**Part VI Suspicious Activity Information - Narrative \*** **3**

Explanation/description of suspicious activity(ies). This section of the report is **critical**. The care with which it is completed may determine whether or not the described activity and its possible criminal nature are clearly understood by investigators. Provide a clear, complete and chronological description (not exceeding this page and the next page) of the activity including what is unusual, irregular or suspicious about the transaction(s), using the checklist below as a guide, as you prepare your account.

- a. Describe conduct that raised suspicion.
- b. Explain whether the transaction(s) was completed or only attempted.
- c. Describe supporting documentation (e.g. transaction records, new account information, tape recordings, E-mail messages, correspondence, etc.) and retain such documentation in your file for five years.
- d. Explain who benefited, financially or otherwise, from the transaction(s), how much, and how (if known).
- e. Describe and retain any admission or explanation of the transaction(s) provided by the subject(s) or other persons. Indicate to whom and when it was given.
- f. Describe and retain any evidence of cover-up or evidence of an attempt to deceive federal or state examiners, SRO, or others.
- g. Indicate where the possible violation of law(s) took place (e.g., main office, branch, other).
- h. Indicate whether the suspicious activity is an isolated incident or relates to another transaction.
- i. Indicate whether there is any related litigation. If so, specify the name of the litigation and the court where the action is pending.
- j. Recommend any further investigation that might assist law enforcement authorities.
- k. Indicate whether any information has been excluded from this report; if so, state reasons.
- l. Indicate whether U.S. or foreign currency and/or U.S. or foreign negotiable instruments) were involved. If foreign, provide the amount, name of currency, and country of origin.
- m. Indicate "Money wire transfer" and "Wire transfer identifier" information when appropriate.
- n. Indicate whether funds or assets were recovered and, if so, enter the dollar value of the recovery in whole dollars only.
- o. Indicate any additional account number(s), and any foreign bank(s) account number(s) which may be involved.
- p. Indicate for a foreign national any available information on subject's passport(s), visa(s), and/or identification card(s). Include date, country, city of issue, issuing authority, and nationality.
- q. Describe any suspicious activities that involve transfer of funds to or from a foreign country or transactions in a foreign currency. Identify the country source and destinations of funds.
- r. Describe subject(s) position if employed by the financial institution.
- s. Indicate whether securities, futures, or options were involved. If so, list the type, CUSIP number or ISIN number and amount.
- t. Indicate the type of institution filing this report, if this is not clear from Part IV. For example, an IA that is managing partner of a limited partnership that is acting as a hedge fund that detects suspicious activity tied in part to its hedge fund activities should note that it is operating as a hedge fund.
- u. Indicate, in instances when the subject or entity has a CRD or NFA number, what that number is.
- v. If correcting a prior report filed in Item I checked, complete the form in its entirety and note the corrected items here in Part VI.

Information already provided in earlier parts of this form need not necessarily be repeated if the meaning is clear.  
**Supporting documentation should not be filed with this report.** Maintain the information for your files.

Tips on SAR form preparation and filing are available in the SAR Activity Review at [www.fincen.gov/pub\\_reports.html](http://www.fincen.gov/pub_reports.html)  
 Enter explanation/description in the space below. Continue on the next page if necessary.

Empty rectangular box for the Suspicious Activity Report Narrative.

**Safe Harbor Federal law (51 U.S.C. 5518(g)(8))** provides complete protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to this report's instructions or are filed on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees, and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure."

**Notification Prohibited Federal law (51 U.S.C. 5518(g)(2))** provides that a financial institution, and its directors, officers, employees, and agents who, voluntarily or by means of a suspicious activity report, report suspicious transactions to the government, may not notify any person involved in the transaction that the transaction has been reported.

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the financial institution shall immediately notify by telephone an appropriate law enforcement authority in addition to filing a timely suspicious activity report.

#### When to file a report

1. Every broker or dealer in securities (BD), futures commission merchant (FCM), and introducing broker in commodities (IB-C) within the United States shall file with FinCEN, to the extent and in the manner required by 31 CFR 105.19 and 105.17, a report of any suspicious transaction relevant to a possible violation of law or regulation. A BD, FCM, or IB-C may also file with FinCEN a report of any suspicious transaction that it believes is relevant to the possible violation of any law or regulation but whose reporting is not required by 31 CFR 105.19 or 105.17. A voluntary filing does not relieve a BD, FCM, or IB-C from the responsibility of complying with any other reporting requirements imposed by the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), a self-regulatory organization ("SRO") (as defined in section 3(a)(26) of the Securities Exchange Act of 1934, 15 U.S.C. 78c (a)(26)), or any registered futures association (RFA) or registered entity (RE) as these terms are defined in the Commodity Exchange Act (CEA) 7 U.S.C. 21 and 7 U.S.C. 1a(29).

2. A transaction requires reporting if it is conducted or attempted by, at, or through a BD, FCM, or IB-C, it involves or aggregates funds or other assets of at least \$5,000, and the BD, FCM, or IB-C knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

i. Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

ii. Is designed, whether through structuring or other means, to evade any requirements of 31 CFR 105 or of any other regulations promulgated under the Bank Secrecy Act, Pub. L. 91-508, as amended, codified at 12 U.S.C. 1829b, 12 U.S.C. 1951-1959, and 51 U.S.C. 5511 - 5514, 5516 - 5522;

iii. Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the BD, FCM, or IB-C knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or

iv. Involves use of the BD, FCM or IB-C to facilitate criminal activity.

5. The obligation to identify and properly and timely report a suspicious transaction rests with each BD, FCM, and IB-C involved in the transaction, provided that no more than one report is required to be filed by any of the BDs, FCMs, or IB-Cs involved in a particular transaction so long as the report filed contains all relevant facts.

4. A SAR-SF shall be filed no later than 90 calendar days after the date of the initial detection by the reporting BD, FCM, or IB-C of facts that may constitute a basis for filing a SAR-SF. If no suspect is identified on the date of such initial detection, a BD, FCM, or IB-C may delay filing a SAR-SF for an additional 90 calendar days to identify a suspect, but in no case shall reporting be delayed more than 60 calendar days after the date of such initial detection. In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, the BD, FCM, or IB-C shall immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a SAR-SF. BDs, FCMs, or IB-Cs wishing voluntarily to report suspicious transactions that may relate to terrorist activity may call FinCEN's Financial Institutions Hotline at 1-866-556-5974 in addition to filing timely a SAR-SF. The BD, FCM, or IB-C may also, but is not required to, contact the SEC or the CFTC to report in such situations.

5. Exceptions. A BD, FCM, or IB-C is not required to file a SAR-SF to report:

i. A robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities, or for lost, missing, counterfeit, or stolen securities with respect to which the BD files a report pursuant to the reporting requirements of 17 CFR 240.17a-1;

ii. A violation otherwise required to be reported on a SAR-SF, (a) of any of the federal securities laws or rules of an SRO by the BD or any of its officers, directors, employees or other registered representatives, other than a violation of 17 CFR 240.17a-5 or 17 CFR 405.4, so long as such violation is appropriately reported to the SEC or an SRO; or (b) under the CEA (7 U.S.C. 1 et seq.), the regulations of the CFTC (17 CFR Chpt.1), or the rules of any RFA or RE as those terms are defined in the CEA, 7 U.S.C. 21 and 7 U.S.C. 1a(29), by the FCM or IB-C or any of its officers, directors, employees or associated persons, other than a violation of 17 CFR 42.2 as long as such violation is appropriately reported to the CFTC or a RFA or RE.

6. The Bank Secrecy Act requires financial institutions to file currency transaction reports (CTRs) in accordance with the Department of the Treasury's implementing regulations (31 CFR Part 105). These regulations require a financial institution to file a CTR whenever a currency transaction exceeds \$10,000. If a currency transaction exceeds \$10,000 and is suspicious, the institution must file both a CTR (reporting the currency transaction) and a suspicious activity report (reporting the suspicious aspects of the transaction). If a currency transaction is \$10,000 or less and is suspicious, the institution should only file a suspicious activity report. Appropriate records must be maintained in each case.

See: 31 CFR Part 105; 17 CFR 240.17a-5; 17 CFR 405.4; 17 CFR 42.2

#### General Instructions

##### A. Abbreviations and Definitions

1. AKA-- also known as (individual)
2. ASE-- American Stock Exchange
3. BD-- Broker or Dealer in Securities
4. CBOT-- Chicago Board Options Exchange
5. CBOT-- Chicago Board of Trade
6. CMEX-- Chicago Mercantile Exchange
7. CPO-- Commodity Pool Operator
8. CRD-- Central Registration Depository
9. CFTC-- Commodity Futures Trading Commission
10. CTA-- Commodity Trading Advisor
11. CUSIP-- Committee on Uniform Securities ID Procedures
12. DEA-- Drug Enforcement Administration doing business as (entity)
13. DBA--
14. EIN-- Employer Identification Number
15. EUREX-- European Exchange
16. FBI-- Federal Bureau of Investigation
17. FCM-- Futures Commission Merchant
18. IA-- Investment Adviser
19. IB-C-- Introducing Broker-Commodities
20. ICE-- Immigration & Customs Enforcement
21. IRS-- Internal Revenue Service
22. ITIN-- Individual taxpayer ID number
23. ISIDP-- International Securities ID Directory
24. KCBOT-- Kansas City Board of Trade
25. LIFFE-- London International Financial Futures Exchange

26. MATIF--	Marche a Terme International de France
27. MCEX--	Mississippi Grain Exchange
28. NASD--	NASD
29. NASDAQ--	Nasdaq Stock Market
30. NFA--	National Futures Association
31. NYBOT--	New York Board of Trade (CSCC, CTN, FINE, NYFE)
32. NYMEX--	New York Mercantile Exchange
33. NYSE--	New York Stock Exchange
34. NYLY--	Nasdaq Life Markets
35. OTC--	Over-the-counter
36. PCX--	Pacific Exchange
37. PHLX--	Philadelphia Stock Exchange
38. RE--	Registered Entity
39. RFA--	Registered Futures Association
40. SEC--	Securities and Exchange Commission
41. SRO--	Self-Regulatory Organization
42. SSN--	social security number
43. USFE--	U. S. Futures Exchange

#### 5. How to make a report:

1. This form can be e-filed through the Patriot Act Communications System (PACS). Go to <http://pacs.fincen.gov> to register. This form is also available for download on the Financial Crimes Enforcement Network's Web site at [www.fincen.gov](http://www.fincen.gov), or may be ordered by calling the IRS Forms Distribution Center at (800) 829-6676. Send each completed suspicious activity report to:

Detroit Computing Center  
Attn: SAR-SF  
P.O. Box 33980  
Detroit, MI 48232

2. Items marked with an asterisk (\*) are considered critical and **must be completed if known**.

3. If the information for a critical item is not known or not applicable, enter special responses "None," "Not Applicable," "Unknown," or "00" (state/country/middle initial) as appropriate to complete the item.

4. Complete each suspicious activity report by providing as much information as possible on initial and corrected reports.

5. Do not include supporting documentation with the suspicious activity report filed. Identify and retain a copy of the suspicious activity report and all supporting documentation (e.g. transaction records, new account information, tape recordings, e-mail messages, correspondence, etc.) or business record equivalent for your files for five (5) years from the date of the suspicious activity report. All supporting documentation must be made available to appropriate authorities upon request.

6. If more than one subject is being reported, make a copy of page 1, complete only the subject information in Part I, and attach the additional page(s) behind page 1. If more space is needed to complete any other item(s), identify that item in Part VI by "item number," and provide the additional information.

7. Type or complete the report using block written letters.

8. Enter all dates in MM/DD/YYYY format where MM=month, DD=day, and YYYY=year. Precede any single number with a zero, i.e., 01/02, etc.

9. List all Telephone numbers with (area code) first and then the seven numbers, using the format (XXX) XXX-XXXX. List international telephone and fax numbers in Part VI.

10. Always enter an individual's name by entering the last name, first name, and middle initial (if known). If a legal entity is listed, enter its name in the last name field.

11. Enter all identifying numbers (alien registration, Corporate/Partnership Resolution, CRD, CUSIP<sup>®</sup> driver's license/state ID, EIN, ITIN, Foreign National ID, IGID,<sup>®</sup> NFAID, passport, SEC, and SSN, etc.) starting from left to right. Do not include spaces, dashes, or other punctuation.

12. Enter all Post Office ZIP codes with at least the first five numbers (at nine (ZIP + 4) if known) and listed from left to right.

13. Enter all monetary amounts in U.S. Dollars. Use whole dollar amounts rounded up when necessary. Use this format: \$0,000,000.00. If foreign currency is involved, state name of currency and country of origin in Part VI.

14. Addresses, general. Enter the permanent street address, city, two letter state/territory abbreviation used by the U.S. Postal Service, and ZIP code (ZIP+4 if known) of the individual or entity. A post office box number should not be used for an individual, unless no other address is available. For an individual, also enter any apartment number or suite number, road or route number. If a P.O. Box is used for an entity, enter the street name, suite number, and road or route number. If the address of the individual or entity is in a foreign country, enter the city, province or state, postal code, and the name of the country (country codes may be found at [www.fincen.gov/reg\\_basforms.html](http://www.fincen.gov/reg_basforms.html)). Complete any part of the address that is known, even if the entire address is not known. If from the United States, leave country item blank.

#### C. Specific Suspicious Activity Report Preparation Instructions

Item 1-- Type of report. Check box if this report is filed to correct a previously filed SAR-SF. To correct a report, a new SAR-SF must be completed in its entirety. Note corrected items in Section VI (see line "c").

#### Part I Subject Information

Note: Enter information about the person(s) or entity involved that caused this report to be filed, not the victim of the activity.

Item 2 -- Multiple Subjects. Check box (a) if multiple subjects are involved. Attach additional copy(ies) of Part I to this report for each subject. Check box (b) if subject information unavailable.

Items 3, 4, and 5--Name of Subject. See General Instruction B10. If the organization is operated under a different trade or business name than its legal name, enter the organization's legal name in Item 3 (e.g., Smith Enterprises, Inc.) and the

name of the business in Item 5 (e.g., Smith's Tavern). If more than one Part I is required, make a copy of page 1 and provide the additional information.

Item 6-- Also known as, or doing business as. If a reporting institution has knowledge of a subject's separate "AKA" and/or entity's "DBA" name, enter it in Item 6.

Item 7-- Occupation/type of business. If known, identify the occupation, profession, or business that best describes the individual in Part I (e.g., attorney, car dealer, carpenter, doctor, farmer, plumber, truck driver, etc.). Do not use non-descript terms such as businessman, merchant, store owner (unless store's name is provided). If self employed, unemployed, or retired are used, add current/former profession if known (e.g. self-employed building contractor, unemployed teacher, retired attorney, etc.). If the individual's business activities can be described more fully, provide the additional information in Part VI.

Items 8, 9, 10, 11, and 12-- \*Address. See General Instructions B12 and B14.

Item 13-- E-mail address. Enter the subject's E-mail address if available.

Item 14-- \*SSN/ITIN (individual) or EIN (entity). See General Instruction B11 and definitions. If the subject named in Items 5 through 8 is a U.S. Citizen or an alien with a SSN, enter his or her SSN in Item 14. If that individual is an alien who has an ITIN, enter that number. If the subject is an entity, enter the EIN.

Item 15-- \*Account number(s). See General Instruction B11. Enter up to four affected account numbers (in or through which the suspicious activity occurred. If no account number is affected leave Item 15 blank. Check the "yes" box to indicate if the account is closed. If more than four accounts are affected, provide the additional information in Part VI.

Item 16-- Date of birth. See General Instruction B5. If an individual is named in Items 5 through 8, enter the date of birth. If the month and/or day is not available or unknown, fill in with zeros (e.g., \*01/00/1989" indicates an unknown date in January, 1989).

Item 17-- \*Government issued identification. See General Instruction B11. Check the appropriate box showing the type of document used to verify the subject's identity. Box "d" denotes that a corporate or partnership resolution was used to identify an entity. If you check the "Other" box "e", be sure to specify the type of document used. In box "f", list the ID number of the identifying document. In box "g", list the issuing authority.

Items 18 & 19-- Telephone numbers. See General Instruction B9. List any additional number(s) (e.g., hotel, cell, etc.) in Part VI.

Item 20-- Institution association. Indicate whether the subject identified in Part I is, or was, associated with the reporting institution as an "associated person," as defined in section 3(a)(18) of the Securities Exchange Act of 1934 or CFTC rule 1.5(a), or is, or was, "affiliated with" the reporting



institution, as defined in the CFTC rule 4.7(a)(1)(ii). If so, explain in Part VI.

#### Part II Suspicious Activity Information

Item 21-- "Date or date range of suspicious activity. See General Instruction B8. Enter the date of the reported activity in the "Item" field. If more than one day, indicate the duration of the activity by entering the first date in the "Item" field and the last date in the "to" field. If the same individual or organization conducts multiple or related activities within the 30 calendar day period after the date of initial detection, the reporting institution may consider reporting the suspicious transactions on one form, but only if doing so will fully describe what has occurred. A new report must be filed for other related suspicious transactions committed after the initial detection period.

Item 22-- "Total dollar amount. See General Instruction B18. Enter the total dollar value of the funds or assets involved in the suspicious activity that is conducted by the same individual or organization within the 30 calendar day period after the date of initial detection. For multiple or related suspicious transactions, show the breakdown of this aggregated total in Part VI. For abuse by a person associated with the institution, the value of this item can be zero (0). Do not use any words, such as "thousand", "million", etc. For foreign currency, convert to U.S. Dollars.

Item 23-- Instrument type. Mark the type of instrument identified in Item 23. (Check all that apply.) In Item 23b, indicate U.S. Dollars only. For Item 23c, indicate currency if other than U.S. Dollars. For Item 23d, enter appropriate three or four letter code.

Items 24, 25, 26, 27, 28, and 29-- CUSIP# Numbers. Enter up to six (6) securities numbers. If more, enter additional in Part VI.

Item 30-- "Type of suspicious activity. Check the boxes that identifies the suspicious activity. More than one box may be checked. Provide a brief explanation in Part VI of why each box is checked. If none of these items applies, mark "other" and provide in Part VI an explanation of the type of suspicious activity.

#### Part III Law Enforcement or Regulatory Contact Information

Items 31, 32, and 33-- Contacting enforcement authorities. If no contact, go to Part IV. See General Instructions "A. Abbreviations and Definitions" for law enforcement and regulatory identities. If you have advised any law enforcement au-

thority SRO, RFA, or RC-futures entity of the suspicious transactions by telephone or written communication, complete this section. If box "b" or boxes "f" through "j" are checked, provide the name of the authority contacted in Item 32. If no contact, leave items 31-35 blank.

Item 34-- Telephone number of individual contacted. See General Instruction B9 for format.

Item 35-- Date contacted. See General Instruction B8 for format.

#### Part IV Reporting Financial Institution Information

Item 36-- "Name of financial institution or sole proprietorship. Enter the full legal name of the institution, i.e., the name shown on the charter or other document creating the entity and registered with the SEC or CFTC. If a sole proprietor, enter the business name of the proprietorship registered with the SEC or CFTC.

Item 37-- "Employer identification number. See General Instruction B11. Enter the reporting financial institution's EIN. If sole proprietor enter SSN or ITIN.

Items \*38, \*39, \*40, and \*41-- Address. See General Instruction B14. This address should be of the principal office or headquarters in the United States.

Items 42, 43, 44, 45 and 46-- Additional address locations. See General Instruction B14. If more than one location is involved, e.g., branch office etc., provide the address of the location where the most significant portion of the suspicious transactions occurred. If more than two locations are involved check box 43 and list locations in Part VI.

Item 47-- Central Registration Depository number. See General Instruction B11. If none, leave blank.

Item 48-- SEC number. See General Instruction B11. This is a ten digit number including the prefix of either "8" or "008" depending on the system used. If none, leave blank.

Item 49-- NFA identification number. See General Instruction B11. If none, leave blank.

Item 50-- Dual reporting. If this is a coordinated report involving more than one individual/entity (see "When to file a report Item 3") check the appropriate box and provide the details in Part VI.

Item 51-- Type of reporting institution. Check all boxes that apply to the particular report. If none of these categories apply to you, explain in Part VI. The Federal Bureau of Public Debt, its agents, and any other federal agency issuers of Federal Securities should mark "U.S. Government broker/dealer." State or municipal issuers of municipal securities should mark "Municipal broker/dealer." A securities SRO, RFA, or RC-futures entity filing this form should identify the institution type as that of the member institution for which this report is being filed, and in Part V, Items 52, 53, 54, 55, 56, and 57) identify the securities SRO, RFA or RC-futures entity individual to contact.

Part V Contact for assistance

Items 52, 53, and 54-- "Contact individual. See General Instruction B10.

Item 55-- "Title/Position. Enter the job title/position of the contact individual.

Item 56-- "Work telephone number. See General Instruction B9.

Item 57-- "Date report prepared. See General Instruction B8.

Part VI " Suspicious Activity Information - Narrative. See page 3 of the form for instructions.

#### Paperwork Reduction Act Notice:

The purpose of this form is to provide an effective means for financial institutions to notify appropriate law enforcement agencies of suspicious transactions that occur by, through, or at the financial institutions. This report is required by law, pursuant to authority contained in 31 U.S.C. 5318(j). Information collected on this report is confidential (31 U.S.C. 5318(i)). Federal securities and futures regulatory agencies and the U.S. Departments of Justice and Treasury, and other authorized authorities may use and share this information. Public reporting and recordkeeping burden for this form is estimated to average 45 minutes per response, and includes time to gather and maintain information for the required report, review the instructions, and complete the information collection. Send comments regarding this burden estimate, including suggestions for reducing the burden, to the Office of Management and Budget, Paperwork Reduction Project, Washington, DC 20503 and to the Financial Crimes Enforcement Network, Attn.: Paperwork Reduction Act, P.O. Box 59, Vienna VA 22183-0059. The agency may not conduct or sponsor, and an organization (or a person) is not required to respond to, a collection of information unless it displays a currently valid OMB control number.