To: Program Administrators ("PA"s) doing business with AIG Property Casualty U.S. ("AIG PC")

From: AIG PC U.S. Compliance Department ("AIG Compliance")

Subject: Anti-Money Laundering Program for Program Administrators

Date: November 24, 2014

As a PA providing services to AIG PC for underwriting and policy issuance, and pursuant to your Program Administrator Agreement ("PA Agreement"), AIG expects you to conduct business in full compliance with all applicable laws and regulations, and AIG policies, including the provisions in the American International Group, Inc., Third Party Code of Conduct ("Code of Conduct").

You are required by your PA Agreement to comply with AIG's Anti-Money Laundering Policy as applicable to a PA. To provide further guidance with respect to our compliance requirements, AIG PC has created an Anti-Money Laundering Program for the PA's use. Elements of the Anti-Money Laundering Program must be incorporated into your company's standard operating procedures and written guidelines with respect to the business administered on behalf of AIG PC.

As per the attached, if you become aware of any potential Anti-Money Laundering issue you must immediately notify your AIG Relationship Manager and AIG Compliance at aigpc.us.compliance@aig.com. Please continue to direct your day to day business questions and inquiries to your AIG Relationship Manager.

Attachments:

- Anti-Money Laundering Red Flag Identification for AIG Business Partners
- AIG Third Party Code of Conduct

Policy Statement	This policy statement summarizes the Anti-Money Laundering Program for PAs. We require all PAs to prohibit and actively pursue the detection and prevention (and, if applicable, the escalation and reporting) of any activity that facilitates money laundering or the funding of terrorist or criminal activity. These procedures apply to all United States based employees of PAs that provide services to AIG PC.
AML Program Control – Red Flag and Suspicious Activity Identification	**Money Laundering Red Flags / Suspicious Activity Indicators** Attached to this document is a list of red flags and suspicious activity indicators which, if present, may raise concerns that there is an attempt to launder money or to finance terrorist activity. All employees of PAs dealing with front-end underwriting, handling payments and processing claims must be made aware of these indicators and, if suspicious activity is identified, further investigate the facts. If a concern still remains after further investigation, AIG Compliance and, simultaneously, the AIG Relationship Manager should be contacted immediately and all further transactions on the policy should cease, including but not limited to paying claims, making a refund payment, and binding, renewing or cancelling the policy. The list of red flags is not meant to be an exhaustive list of suspicious activities and the occurrence of such activity does not constitute evidence of wrongdoing.
AML Program Control – Underwriting Customer Due Diligence/ Know Your Customer	Each PA shall, at a minimum, obtain the below information during the underwriting process to comply with the customer data collection requirements. The scope of customer information that needs to be obtained varies between the Commercial and Consumer businesses as follows: Commercial* • Name of the company • Nature of the business activity • Information sufficient to assess the risk hazards • Location(s) and address(es) * AIG has specific Know Your Customer (KYC) and screening requirements for Ocean Marine coverage. If you are handling Ocean Marine coverage, please discuss these requirements with your Relationship Manager. Consumer • Name and/or names on the policy • Address • Contact number (if applicable) *For coverages such as No Additional Charge (NAC), group travel, and warranty, underlying insureds may or may not be disclosed in the normal course of business. When and if such insureds are identified, this information must be screened in accordance with the PA Agreement.
AML Program Control – Transactions	• Premium Collections — Acceptance of payments via cash may be evidence of suspicious activity and must be avoided where possible in the conduct of business. The use of electronic or other such funds transfer mechanisms is preferred. **In the event a PA is determined to have accepted cash in excess of $10,000, AIG Compliance must be notified immediately**. • Policy Cancellations — PAs shall review voluntary early policy cancellations where premium is refunded to determine if any suspicious activity exists. • Payments — PAs will not pay claims or issue any other payments without the required screening of the beneficiaries.

Suspicious Activity Handling Requirements/ Internal Reporting	The following outlines how identified suspicious activity must be handled: • **Do not proceed**. Employees of PAs must further investigate facts to ensure that any suspicious activity is resolved prior to binding a policy or paying a claim; • After completing a diligent review of the facts, if money laundering or terrorist financing is still suspected, employees of PAs must contact both their AIG Relationship Manager and AIG Compliance; and • AIG Compliance will be responsible to see the matter to completion, including directing the collection of relevant information from the PA, business unit and/or functional area.
Government Information Requests	An employee of a PA who receives a subpoena or other request for information (as it relates to an AIG policy, program or business venture) from any governmental authority, law enforcement agent, regulator, attorney or member of the media suggesting criminal or unlawful activity by a customer must adhere to the following: • **Immediately** notify their Relationship Manager and AIG Compliance. • Not discuss the request with anyone other than their Relationship Manager and AIG Compliance; and • Direct all subsequent requests to AIG Compliance at aigpc.us.compliance@aig.com for further handling.
Prohibited Disclosures	It is important that employees of PAs must not "tip off" or advise a customer or any other person that the customer, customer's account(s) or other customer relationships are being reviewed as a result of potentially unusual or suspicious behavior. Under no circumstance may a customer be told that the customer is or was the subject of an internal investigation. What is permissible and can be conveyed to the customer: • "the account/transaction is being reviewed against internal procedures at the moment, we will advise you when this has been completed" • "I apologize, I am not allowed to comment on our internal processes" What is prohibited from being conveyed to the customer: • "the transaction is being or was delayed because a Suspicious Activity Report was filed"; • "the transaction has been or will be reported to a governmental or other regulatory authority"; and • "the Customer" is being investigated by law enforcement agencies"
Record Retention	Records must be retained in accordance with the requirements of the PA Agreement. Please contact your AIG Relationship Manager with any related questions.
Updates	Version 1 November 24, 2014

Anti-Money Laundering Red Flag Identification for AIG Business Partners

If any of these Red Flags are identified and still considered suspicious after investigation contact your relationship manager as well as AIG PC US Compliance at **AIGPC.US.COMPLIANCE@aig.com**.

Underwriting

- Policyholder is hesitant, provides minimal or seemingly false information, or delays, refuses, or appears reluctant to provide required information when requested.
- Policyholder identity is not disclosed where disclosure of principal is required by the business (i.e. an agent not disclosing his principal).
- Policyholder voluntarily requests early cancellation, especially at a significant cost to the customer, resulting in a refund of premium and does not provide proper explanation or justification or the refund check is directed to an apparently unrelated third party.
- Policyholder requests insurance that is not consistent with customer's needs and/or outside the customer's normal pattern of business.
- Policyholder requests coverage or limits greater than the risk exposure that generates a higher premium and/or seems indifferent to paying premium that exceeds fair market value.
- Policyholder shows little or no concern for the value or benefits of the insurance product, but shows much concern about early termination features.
- Policyholder requests coverage for a business or high value personal asset yet there is a refusal or inability to supply sufficient information about the business, need for coverage, etc.

Claims

- Claimant is reluctant or unable to provide all requested claims information, refuses to meet the claims representative at the claimant's residence or place of business, or requests to meet at odd hours.
- Claimant requests the claim be paid in a different country or in a different currency from the premium.
- Claim circumstances do not make sense, given the nature of the customer's business.

NOTE: All suspected claims fraud must be escalated to your relationship manager who, if applicable, will engage the appropriate AIG personnel. If the fraud is suspected to be motivated by intent to launder money or finance terrorism notify AIG PC U.S. Compliance and your relationship manager immediately.

Collections

- Policyholder proposes payment to be made in cash.
- Policyholder significantly overpays premium which is immediately followed by a request for a refund of overpayment.

For further information about Anti-Money Laundering please contact your relationship manager.