PROGRAM ADMINISTRATOR

LEGAL COMPLIANCE MANUAL

U.S. DOMESTIC EDITION

Edition Date: January 2020

TABLE OF CONTENTS

I. INTRODUCTION

The reputation and success of the U.S. domiciled member companies of American International Group, Inc. (hereinafter referred to collectively as "AIG" or the "Company" and listed in Appendix A) depends on compliance with all applicable state and federal laws and regulations**.** Any conduct that would violate these laws and regulations may have a negative impact on both the Company's reputation and financial interests. Accordingly, the Company demands from its Program Administrators the highest degree of integrity, ethical behavior and regulatory compliance in providing products and services on behalf of the Company.

Under the McCarran-Ferguson Act, the primary responsibility for regulating the insurance industry lies with the states. Each state maintains its own insurance department and workers' compensation board, which promulgate insurance laws and regulations according to its own public policy. Accordingly, the laws and regulations relating to any given area of insurance may differ from state to state.

For example, each state, through its Department of Insurance, has established rules and regulations regarding the handling of insurance contracts. These rules and regulations relate to issues including, but not limited to, timeliness in policy issuance; cancellation and non-renewal procedures[1] and adherence to filed and approved forms and rates. Program Administrators have an obligation to keep abreast of and follow these rules and regulations.

Other examples of regulatory compliance issues include, but are not limited to, the following: Cancellation or non-renewal of the Companies' policies must be done in compliance with the cancellation and non-renewal procedures set forth in each insurance policy and any applicable law or regulation. Failure to comply with cancellation and non-renewal requirements may render the cancellation or non-renewal ineffective and may also subject the Company to regulatory sanctions.

Policies cannot be canceled or non-renewed because of the policyholder's race, color, religion, sex or national origin. Additional categories of protected classes may exist under state laws or regulations, such as ancestry, sexual orientation, HIV status, marital status, age, disability, sickle cell trait, certain preexisting conditions, breast cancer and victims of domestic violence. Some states also prohibit discrimination based on the results of genetic testing.

The insurance laws and regulations of each state, with several significant exceptions, require insurers issuing policies of insurance on an admitted basis to obtain approval for such insurance policies (*i*.e., forms, rates and rules) prior to their use. Accordingly, no form, rate or rule may be used unless it has been approved by the AIG Program Manager responsible for the program, the AIG Legal Department counsel and, where required, by the appropriate state regulatory authority.

Insurance department consumer complaints must be submitted to the AIG Program Manager responsible for the program who will forward it to the AIG Legal Department.

[1] Cancellation or non-renewal of the Companies' policies must be done in compliance with the cancellation and non-renewal procedures set forth in each insurance policy and any applicable law or regulation. Failure to comply with cancellation and non- renewal requirements may render the cancellation or non-renewal ineffective and may also subject the Company to regulatory sanctions.

Compliance with the applicable legal and regulatory state filing requirements is critical to the Company's ability to enforce policy terms or collect premiums and in the event of non- compliance may subject the Company to regulatory fines and other sanctions.

However, a degree of uniformity has been achieved among the states through the efforts of the National Association of Insurance Commissioners (NAIC) where many states have adopted some form of the NAIC model acts. In addition, there are several federal laws that affect and regulate the activities of insurance companies. Additionally, while the insurance industry is regulated primarily by the states, there are also federal laws that affect the activities of all companies, including insurance companies and insurance agencies. Federal laws governing issues such as telemarketing, civil rights, insurance fraud and privacy may be applicable to Program Administrator activities. As independent contractors of the Company, Program Administrators must be aware that their activities are subject to, and must comply with, both state and federal legal/regulatory requirements.

The Program Administrator is also responsible for adhering to the Program Administrator Agreement, which is the contract that sets forth the relationship between the Company and the Program Administrator and the Company's expectations.[2] Failure to comply with statutes or regulations involving the handling of insurance contracts may violate the Program Administrator Agreement and subject the Program Administrator to cancellation as an approved representative of the Company. It is the obligation of all Program Administrators to report to the Company any failure to abide by any governmental, regulatory or compliance matter including any complaints or hearing notices received from any state insurance department.

Attorneys in the AIG Legal Department provide advice to AIG businesses on legal, regulatory and compliance issues. The AIG Legal Department and AIG Compliance work with AIG businesses to achieve and maintain compliance with internal, regulatory and bureau mandated requirements, consistent with Company objectives and business plans. Any questions regarding any issue involved in this manual should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate a response with the AIG Legal Department or AIG Compliance.

This Regulatory and Compliance Manual (the "Compliance Manual") is not intended to provide legal advice nor does it encompass every law, regulation and procedure that Program Administrators should follow. Rather, this Compliance Manual sets forth certain regulatory and compliance issues and requirements established by the Company. It is recommended that each Program Administrator establish its own compliance program.

[2] If there is any conflict between this manual and the Program Administrator Agreement, the terms of the Program Administrator Agreement will govern.

II. ADVERTISING & BRANDING

Insurance advertising is subject to state and federal laws and regulations. Unfair or deceptive advertising is prohibited and can have significant adverse civil and regulatory consequences. The Company requires that advertising done on its behalf be truthful in all respects.

Advertising may be broadly defined as any material designed to (a) create public interest in insurance, an insurance company, or an insurance product or (b) induce the public to purchase, increase, modify, reinstate, borrow on, surrender, replace or retain an insurance policy. Advertising includes printed, published and audiovisual material, social media, descriptive literature used in direct mail, newspapers, magazines, radio, television, billboards and similar displays, and material available on the Internet or in other electronic formats. It also includes descriptive literature and sales aids of all kinds (*e.g.*, letterhead and business cards) and materials used for prepared sales presentations (including telephone scripts and seminar materials), among other items.

The form that advertisements may take, what information is required or permissible to be disclosed, and what information may not be disclosed may be specifically regulated. The use of the Internet to sell insurance is regulated by federal and state statutes and regulations relating to advertising.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. AIG and its subsidiaries and affiliates have established brands and trademarks that need to be protected. The AIG brand and those of its subsidiaries' and affiliates' (including any trademarks owned by such entities) may not be used by Program Administrators without express written permission of AIG Legal Department. If a Program Administrator wishes to use AIG's trademark on its website, it must execute a Trademark License agreement with AIG, which can be obtained through the AIG Program Manager.

Questions regarding advertising or branding should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

III. MARKETING & TRADE PRACTICES

A. MARKETING

1. Marketing Materials

Marketing materials that describe AIG's products and services must be truthful and accurate in all respects as well as appropriate for the intended audience. All such marketing materials (including commercial e-mails) are subject to prior review and approval by the AIG Legal Department. The AIG Program Manager responsible for the program will coordinate such approval with the Program Administrator and the AIG Legal Department. (See Chapter II. of this Manual regarding Advertising & Branding)

2. Commercial E-mail

Federal laws (in particular, the CAN-SPAM Act of 2003) and state laws regulate *commercial e-mail* and, generally: (1) require senders of *commercial e-mail* messages to provide recipients with an opportunity to opt-out from receiving additional e-mails from the sender; and (2) prohibit e-mail practices that are fraudulent or deceptive in nature. A *commercial e-mail* is an e-mail message, the primary purpose of which is the commercial advertisement or promotion of a commercial product or service. *Commercial e-mail* includes newsletters, invitations to events, articles and press releases where the Program Administrator promotes the Company's products or services. It is the policy of the Company, as set by the AIG Chief Privacy Officer, that: (1) commercial e-mails may be sent to AIG Commercial Insurance's insureds or potential insureds; however, such activity must be coordinated in advance through the AIG Program Manager responsible for the program, who will ensure a proper opt-out system is put in place by the Program Administrator; and (2) no commercial e-mails may be sent to insureds or potential insureds without prior notification to the AIG Chief Privacy Officer.

3. Telemarketing

In order to combat telemarketing abuse and fraudulent practices, Congress has given both the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) power to regulate telemarketing. The FTC and FCC regulations generally prohibit deceptive or abusive telemarketing practices, including credit card laundering, intentional harassment, and calling outside of restricted hours.

Accordingly, the FTC and FCC have implemented regulations regarding telemarketing. The federal government now requires any company that utilizes telephone marketing to verify its call list against the National Do Not Call Registry.

Program Administrators are required to follow the guidelines of the National Do Not Call Registry, which can be accessed at www.ftc.gov/donotcall.

States also have statutes and regulations governing telemarketing activities, so telemarketing programs must be tailored with both levels of regulation (state and federal) in mind. States may bring civil actions on behalf of their residents to enjoin state or federal telemarketing violations and to recover for actual monetary loss. The Company is firmly committed to complying with all applicable telemarketing regulations. Failure to comply with both federal and state regulations can result in severe civil penalties, including injunctive relief, restitution and/or substantial fines.

4. Unsolicited Fax Transmissions

Federal regulations require, in most cases, that companies obtain an express invitation or prior permission from a recipient before transmitting an unsolicited fax advertisement. AIG policy prohibits the sending of unsolicited fax advertisements in all cases, even where they may be permitted by law under certain conditions.

Questions regarding this policy should be directed to the AIG Program Manager responsible for the program.

B. TRADE PRACTICES

Federal and state laws and regulations prohibit sales practices considered unfair or deceptive to customers or competitors. These sales practices are commonly referred to as "unfair trade practices." Examples include, but are not limited to:

(1) Misrepresenting or falsely advertising any aspect of an insurance policy;

(2) Any false, deceptive or misleading advertising relating to an insurance company, a competitor or the industry;

(3) Offering to give anything of value to a prospective purchaser as an inducement;

(4) Making any false material statement or entry in any book or report as to the financial condition of an insurance company;

(5) Unlawful discrimination; and

(6) Lending money or extending credit on the condition that the prospective debtor also purchases insurance from the lender.

The use of misleading, false, defamatory or unauthorized information or representations can lead to serious legal consequences. Accordingly, the Company will not tolerate any unfair trade practices used by Program Administrators when acting on its behalf.

IV. CLAIMS PRACTICES

Pursuant to the Program Administrator Agreement, the Program Administrator has no power to negotiate, adjust, compromise, settle or in any way commit the Company to liability with respect to any claim or suit, unless the Program Administrator is authorized to do so by the Company pursuant to a separate claims management agreement (a "Claims Management Agreement"). If the Program Administrator enters into a Claims Management Agreement with the Company, the Program Administrator's claims handling activity will be governed by the Claims Management Agreement.

V. COLLECTIONS

The Company is subject to various legal and regulatory requirements governing its collection practices. Accordingly, Program Administrators must exercise care in ensuring that efforts to collect debts on behalf of the Company are made in accordance with such requirements as well as with the Company's policies.

The primary federal law that governs debt collection is the Fair Debt Collection Practices Act (FDCPA). There are also applicable state laws that regulate debt collection. Program Administrators may not engage in conduct prohibited by any relevant state or federal statutes including, but not limited to:

(1) Using or threatening to use violence or other criminal means to harm the physical person, reputation, or property of any person;

(2) Using obscene or profane language;

(3) Publishing a list of customers who refuse to pay their debts;

(4) Advertising for sale any debt to coerce payment of the debt;

(5) Causing the telephone to ring repeatedly or engaging a person in a telephone conversation with the intent to annoy or harass or without disclosing a caller's identity;

(6) Using any names or insignia to suggest that a governmental department, unit or agency or any third party other than the Company is involved in the collection of the debt;

(7) Falsely representing the character, amount or legal status of the debt, or that the customer is engaged in criminal conduct;

(8) Using false representations or deceptive means to obtain information about a debtor, or threatening to take action that cannot legally be taken or that is not intended to be taken to collect the debt;

(9) Communicating or threatening to communicate to any person credit information that is known or should be known to be false, including the failure to communicate that the debt is in dispute; and

(10) Commencing or causing to be commenced any lawsuit, arbitration or other adversary proceedings in any forum against any individual or corporate entity who allegedly owes a debt without having a good faith or reasonable factual basis for believing that the debt is due and owing.

Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

VI. E-MAIL & INTERNET USE

Generally, when using e-mail or the Internet to advertise, market, solicit or sell products on behalf of the Company, Program Administrators should be cognizant that such activities are subject to state and federal statutes and regulations that are currently evolving. The general rule to follow is that activities over the Internet are regulated in the same manner as they are in the non-Internet environment. However, regulators have recently become more concerned with consumer protection online, especially with respect to privacy, spam, and the use of e-signatures.

Some of the issues Program Administrators should be aware of when considering the use of e-mail and the Internet include the following:

(1) Contact with a consumer in a given state or foreign country via the Internet may be sufficient for governmental authorities in such a locale to establish jurisdiction over an AIG member company or a Program Administrator for purposes of insurance regulation, taxation, or civil or criminal actions;

(2) An Internet advertisement may subject AIG to liability if it is (i) accessed in states or foreign countries where the advertisement does not conform to applicable local law, (ii) misrepresented by another online user (*e.g.*, copied or framed without permission) or (iii) not updated and correct at all times;

(3) Communication with customers by means of a website or e-mail can be subject to federal, state and local laws and regulations governing the collection and use of customer data;

(4) Marketing e-mails and other widely distributed electronic communications may be regulated by federal, state, and local anti-spam laws;

(5) Content related to AIG that appears on a Program Administrator's website, as well as the manner in which producers do business online, may subject such the Company to liability. Program Administrator websites that include Company product information and brands (including names and logos) must be reviewed and approved in advance by the AIG Legal Department;

(6) Use of the Internet may subject AIG or a Program Administrator to liability if the information is accessed in states or foreign countries where an agent, insurance company or broker is not licensed or otherwise authorized to do business, or where the product has not received the required regulatory approval;

(7) If operation of an authorized website maintained on behalf of the Company is outsourced, the contract with the third party vendor must be drafted carefully to ensure that the services provided comply with applicable laws and regulations, as well as Company standards. Many software and service providers are not familiar with insurance laws/regulations and expect the Program Administrator to manage the legalities of website design and operation; and

(8) Many websites provide users with a "click and bind" option. On some websites, the "click and bind" process may allow the user to purchase, pay for and immediately receive a copy of a policy. On other websites, the "click and bind" process may allow the user to receive a quote that is binding under given circumstances. These scenarios, as well as other "click and bind" scenarios, may trigger regulatory issues. Program Administrators using any type of "click and bind" process must have the process, as well as the website content and functionality, reviewed and approved in advance by the AIG Legal Department.

Increased use of social media by a Program Administrator's customers, producers, and employees may also raise additional legal issues. These can include privacy and publicity concerns, intellectual property issues, and compliance questions. Interactions on blogs or social networking sites such as LinkedIn, Facebook, or Twitter should comply with all applicable laws and Company policies, and may be subject to additional restrictions.

Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

VII. FRAUD

Insurance fraud is a serious concern. Industry sources estimate that insurance fraud costs the insurance industry billions of dollars a year.

Most states have enacted insurance anti-fraud statutes and regulations which require insurance carriers to, among other things, (i) implement anti-fraud initiatives and educate employees to detect and report suspected fraudulent insurance activity to the AIG fraud units and (ii) in certain circumstances, report such incidents of suspected fraud to the authorities and/or law enforcement for further investigation and potential prosecution.

The successful pursuit of actual and potential insurance fraud against AIG is extremely important. Not only could it result in AIG being reimbursed for dollars paid as a result of fraud in both criminal and civil proceedings, but a robust and active fraud program simultaneously serves as a strong deterrent for potential future misconduct.

Types of Insurance Fraud

Insurance fraud may occur in any aspect of the insurance business, including the following circumstances:

Underwriting Fraud occurs when an insurance application or supporting documentation contains a material misrepresentation or omission of facts bearing on the nature or extent of the risk for which coverage is sought. It induces an underwriter to rely upon the misrepresentations and issue coverage or certain terms that otherwise would not have been issued had the true facts been known.

Claims Fraud includes circumstances where a claimant has fabricated a loss, or has submitted a legitimate loss but fraudulently exaggerates the nature or extent of the loss or associated damages.

Medical Provider Fraud involves a legitimate or fabricated loss by the claimant, where the provider either fabricates the services provided, bills the carrier for more expensive treatment than was necessary or rendered, or makes referrals to other providers for unnecessary treatments.

Premium Fraud occurs when an insured intentionally misrepresents facts related to the "exposure" upon which the underwriter has calculated, quoted and/or adjusted the premium in order to obtain a lower premium. For example, workers' compensation premium fraud occurs when an insured misrepresents the amount of its remuneration, misclassifies its payroll and/or employees' job functions, and/or misrepresents actual employees as independent contractors in order to exclude them for premium purposes.

Any person connected with a Program Administrator who knows or reasonably suspects that a fraud has or may have been, or is being or is about to be, committed has an obligation to immediately report such fraud directly to the AIG Program Manager responsible for the program, who will in turn immediately contact the AIG Legal Department. This reporting requirement applies to all suspected incidents of fraud, regardless of the dollar amount that may be involved.

Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

VIII. INQUIRIES FROM INSURANCE DEPARTMENTS, POLICYHOLDERS, CLAIMANTS & THE PUBLIC

The Company is committed to both regulatory compensation and providing exemplary customer service. This includes being responsive to the inquiries of insurance departments, other regulatory bodies, policyholders and members of the public. All inquiries from the public must be handled with care to ensure that confidential information is not inadvertently disclosed.

A consumer complaint is any written or verbal communication in which a policyholder, first or third party claimant, or consumer files a grievance expressing dissatisfaction with the services received from the Company. The responsibility of the AIG Legal Department Consumer Complaints Department is to receive and log such grievances and work with the respective business unit(s) to prepare an appropriate written response to the allegations. Responses often must include supporting documentation, *e.g.* copies of claims files, insurance policies, cancelled checks, etc.

When a consumer files a complaint with a Department of Insurance, the Department of Insurance forwards the complaint to the applicable insurance carrier requesting a written response that addresses the allegations raised by the complainant. Time periods and deadlines for response are set forth by state regulation or statute. On average, consumer complaints must be responded to within seven (7) to twenty-one (21) calendar days from receipt. Insurance carriers who fail to comply with the mandated response times may incur penalties by the state, which can include monetary fines and/or required appearances before the Department of Insurance or appropriate regulatory body. Program Administrators must cooperate in a timely, complete and responsive manner with the Company in responding to all regulatory inquiries and consumer complaints.

In the event that the Program Administrator receives a regulatory inquiry or consumer complaint, the Program Administrator must immediately forward it to the AIG Program Manager responsible for the program. The AIG Program Manager will immediately forward the complaint and any related correspondence to the Consumer Complaints Department of the AIG Legal Department for handling. The Program Administrator must, upon request, cooperate with the Company, in accordance with the AIG Global Complaints Handling Policy, and provide all relevant documentation for the Company to respond to the consumer compliant and/or regulatory inquiry.

IX. LOBBYING & POLITICAL ACTIVITIES

Under no circumstances is a Program Administrator authorized to make any political contribution, advocate or lobby any political position on behalf of the Company without the express prior written permission from the Company.

Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

X. PRODUCER LICENSING & APPOINTMENTS

Each state or jurisdiction has licensing requirements for insurance agents and brokers. The Program Administrator is responsible for securing and maintaining all licenses required to operate legally in each state or jurisdiction in which it transacts business, and for ensuring that all sub- agents and sub-producers hold appropriate licenses.

Additionally, states have producer appointment requirements that must be complied with. All Program Administrators must respond promptly to requests from the Company for information regarding state insurance licenses and cooperate with the Company regarding the completion of background checks and all other activities surrounding the appointment process. AIG's Producer Licensing Department (the "PLD") is responsible for processing appointments with the state insurance departments. The Program Administrator is responsible for notifying the PLD of all producers, agents, sub-producers and sub-agents who must be appointed and submit the required documentation to the PLD. The Program Administrator is also responsible for ensuring compliance with any state requirements regarding their relationship with sub-producers and sub-agents including contractual authorization and formal appointments/affiliations.

Failure to comply with such licensing and appointment requirements may subject the Company to regulatory penalties and civil liability. The Program Administrator, pursuant to the Program Administrator Agreement, is responsible for any damages, penalties, fines and liabilities incurred by the Company as a result of any violation.

The Program Administrator shall immediately notify the Company of any lapse, cancellation, suspension or termination of any license necessary to fulfill its duties under its Program Administrator Agreement. Notification of any new employees of the Program Administrator, who require appointment, shall also be provided to the Company.

All laws requiring a resident producer to countersign a policy sold by a non-resident producer have been either repealed or struck down by the courts. There are a few states, however, that still require that the policy be signed by the producer, but the producer may be either a resident or non-resident of the state in which the risk is written.

Questions regarding producer licensing should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

XI. REGULATORY REPORTING

AIG is required to report data to various entities such as departments of insurance and other regulatory bodies that regulate them, as well as statistical agents such as the Insurance Services Office, Inc. (ISO), the National Council on Compensation Insurance (NCCI) and the Surety & Fidelity Association of America. In order for AIG to provide timely and accurate data, they must accumulate and report this data in accordance with certain reporting requirements.

Since some of the data components may originate from Program Administrators, Program Administrators must accurately compile and transmit data to the Company in a manner and format prescribed by AIG so that they can meet its reporting obligations described above.

Occasionally, regulators will request that AIG provide data on an ad hoc and/or voluntary basis. Should a Program Administrator receive such a request, the Program Administrator must immediately notify the AIG Program Manager responsible for the program.

Failure of the Company to accumulate and transmit accurate data can result in damage to the Company and/or the Company's reputation and/or fines and penalties, and in certain situations, the inability of the Company to continue to write business.

XII. STATE & FEDERAL CRIMES

Certain activities involving the insurance industry have become the focus of both state and federal criminal laws. The Company requires that its Program Administrators be alert to the prohibitions set forth in these laws.

The federal Violent Crime Control and Law Enforcement Act of 1994 (the "Act") specifies various acts that constitute federal crimes. These acts may also constitute violations of state criminal statutes. They include: (i) false financial reporting, including false valuation of any property; (ii) embezzlement or misappropriation of money, funds, premiums, credits or property of any insurer; (iii) false entries in the books, records and statements of any insurer; (iv) use of force or threats to corruptly influence, impede or obstruct any insurance regulatory action; and (v) the hiring of and/or participation in the business of insurance by any individual convicted of a felony involving dishonesty or a breach of trust or who has been convicted of an offense under the Act.

The Act also imposes criminal liability on individuals who willfully permit the participation of convicted felons in the business of insurance, as well as criminal and civil penalties against individuals and companies engaging in conduct constituting violations of the Act. Many states require background checks prior to producer licensing and/or appointment. Program Administrators must report any criminal convictions against themselves or any employees or sub- producer to the AIG Program Manager responsible for the program, who will in turn immediately contact the AIG Legal Department.

A pattern of violating certain laws may subject the Company, its employees or Program Administrators to additional civil and criminal liability under federal or state Racketeering Influenced and Corrupt Organizations laws.

The use of inaccurate information, especially financial data, may also give rise to civil, regulatory or criminal liability if the material is distributed through the U.S. mail or other means of interstate commerce, including over the telephone, the Internet or by facsimile.

The Company requires that all Program Administrators comply with all applicable state and federal criminal laws. Any person connected with the Program Administrator who knows or reasonably suspects that a crime has or may have been, or is being or is about to be committed has an obligation to report such information immediately to the AIG Program Manager responsible for the program, who will in turn immediately contact the AIG Legal Department.

Any person who intentionally withholds such information is in violation of the AIG Compliance program. Additionally, a pattern of violating certain laws may subject the Company, its employees or Program Administrators to additional civil and criminal liability under federal or state racketeering laws (*e.g.*, Racketeer Influenced and Corrupt Organizations Act).

XIII. UNLAWFUL DISCRIMINATION

The Company is committed to applying designated underwriting criteria fairly and consistently in all aspects of its businesses. The Company does not permit and will not tolerate unlawful discrimination under any circumstance.

Federal and state laws prohibit discrimination based on several categories, including race, color, religion, sex or national origin.

State laws and regulations also prohibit certain types of discrimination. An example of discrimination that may be prohibited under state laws or regulations includes refusing to issue an insurance policy based on an applicant's sex, marital status (except for the purpose of defining persons eligible for dependent benefits), race, religion or national origin. Redlining, the term used to describe an insurer's refusal to insure consumers who live in certain neighborhoods, is also a form of prohibited discrimination. Accordingly, the Program Administrator must conduct its business in compliance with all applicable anti-discrimination laws.

Additional protected classes under state law or regulation may include ancestry, sexual orientation, HIV status, age, disability, sickle cell trait, certain preexisting conditions, breast cancer and victims of domestic violence. Some states also prohibit discrimination based on the results of genetic testing. Doing business with or issuing insurance to states, municipalities or other government entities may require the Company to adhere to the anti-discrimination directives of that political subdivision or governmental entity. The Program Administrator may <u>not</u> make any representation that the Company is in compliance with such directives. Any certification of such compliance required by the political subdivision or governmental entity can only be made by the Company.

Unlawful discrimination may expose the Company to civil and regulatory liability.

Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

XIV. USE OF CONSUMER CREDIT REPORTS

The Company is subject to various federal and state laws and regulations concerning the use of consumer credit reports in insurance transactions and the distribution of such reports to affiliated entities and others. These laws include the federal Fair Credit Reporting Act (FCRA), state analogues to the FCRA, and state privacy protection laws and regulations.

A "consumer credit report" is any written, oral or other communication of any information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance primarily for personal, family or household purposes, employment or other permissible purposes under the FCRA.

Under federal law, consumer credit reports may be obtained only by persons who intend to use the information in whole or in part: (i) in connection with a credit transaction involving the consumer who is the subject of the report and involving the extension of credit to, or review or collection of the account of, the consumer; (ii) for employment purposes; (iii) in connection with the underwriting of insurance involving the consumer; or (iv) for other legitimate business needs in connection with the business transaction involving the consumer that is not specifically covered in (i)-(iii) above.

Federal law imposes certain disclosure obligations when consumer credit reports are used in whole or in part as a basis for an adverse underwriting or credit decision. Those obligations include disclosure that a consumer credit report was consulted, the name and address of the agency from whom the consumer credit report was obtained and a notice that the consumer has a right to contact the reporting agency to secure a copy of the report.

Certain state analogues to FCRA and privacy laws and regulations impose additional disclosure requirements before and after a consumer credit report is used in underwriting decisions.

Pursuant to the FACT Act of 2003, on 11/9/2007 the Federal Trade Commission (FTC) issued a new Address Discrepancy Rule that requires all users of consumer reports to confirm the identity of the consumer when they receive a credit report with an address discrepancy indicator on it. The purpose of the rule is to enhance the accuracy of consumer reports. The new Address Discrepancy Rule was effective 11/1/2008 and applies to anyone requesting a credit report.

Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

XV. ECONOMIC SANCTIONS

All Program Administrators must comply with the AIG Economic Sanctions Compliance Policy and have written procedures designed to comply with all applicable U.S. sanctions laws. U.S. economic sanctions are administered by the Office of Foreign Assets Control ("OFAC"), a division of the U.S. Department of Treasury, and impose requirements and restrictions on U.S. persons, wherever located.

AIG's domestic insurers are required to comply with U.S. sanctions requirements on a global basis. Accordingly, persons acting on AIG's behalf are prohibited from engaging in the following:

- Business transactions with or involving
  - countries subject to comprehensive U.S. sanctions (Sanctioned Countries)
  - any person or entity domiciled, located or incorporated in Sanctioned Countries
  - any person or entity on OFAC's Consolidated Specially Designated Nationals (SDN) List
  - entities, vessels or aircraft connected to any of the above.

- Providing support in any manner to a non-U.S. person's dealings with or involving any of the above or making business referrals regarding any of the above.

To demonstrate compliance in this area, Program Administrators must have written procedures in order to address the following:

Due Diligence

Prior to binding any insurance on AIG's behalf, a Program Administrator must review the proposed transaction and the involved parties and make a risk-based assessment as to whether the cover or service to be provided might give rise to a potential sanctions issue. Reviews should include consideration of customer submissions, communications and schedules of covered property, routes, vessels, trips and locations.

For commercial insureds, a risk-based inquiry should be conducted into whether a customer has business activities in sanctioned countries. The sanctions assessment must be documented in the underwriting file or otherwise accessible upon request.

Examples of economic sanctions exposures include the following:

- insureds or connected parties who are incorporated, domiciled or located in any of the Sanctioned Countries
- insureds who conduct business in a Sanctioned Country (e.g. operations, investments, services, shipments, sales, supply channels, covered property)
- instances where the underwriting file shows that an insured's board members or officers are domiciled or located in a Sanctioned Country
- instances where the underwriting file shows that an insured is 50% or more owned by Sanctioned Country residents
- coverage involves individuals or entities on any OFAC list
- an insured vessel is located or flagged in a Sanctioned Country

Screening

In addition to the risk-based due diligence mentioned above, a Program Administrator must have a process in place to screen customer and transaction data, including the name and country of residence of each known insured, additional insured, beneficiary, connected party, payee, and processing bank.

Program Administrators must have a sanctions screening process in place that includes screening of customer and transaction data against the following lists:

- OFAC SDN, FSE and SSI lists (see the OFAC Consolidated List published on its website)
- List of cities, towns, and ports of Sanctioned Countries
- Where appropriate, lists of vessels subject to U.S. sanctions (e.g., for the claims process, for hull insurance and for the issuance of marine cargo insurance certificates)

All Program Administrator systems must be configured to store available customer data in a manner that allows screening data in a timely manner.

Prior to providing any payment or service, Program Administrators must screen all potential payees, including third party liability claimants, to determine whether payment or any other benefit would be prohibited by U.S. sanctions laws. To the extent known, all banks involved in an outgoing payment order must be screened. Outbound payments must be screened prior to issuance.

Claims

To the extent that a Program Administrator is processing AIG claims, it must have processes in place to conduct sanctions screening of all AIG claims data. This includes:

(1) Manual review of claims files for references to Sanctioned Countries
(2) Screening of names and countries of residence of all parties connected to a claim
(3) Where vessels are involved, screening of the vessel

During the claims handling process (i.e., following receipt of the claims information), all individuals and entities involved with or having an interest in a claim (including insureds, beneficiaries, claimants, payees, vendors, freight forwarders, vessels, etc.) must be screened.

Where a potential sanctions issue is detected, no claims service or payment can be provided unless and until preapproval from AIG Compliance is given.

Sanctions Exclusionary Language

AIG includes within its policies preapproved sanctions exclusionary language that voids coverage that would violate U.S. sanctions laws and that states that AIG will not pay a claim where prohibited by U.S. sanctions laws. These exclusions must be issued as part of any AIG insurance policy unless there is a documented sanctions assessment indicating that there is no sanctions exposure. Any request to omit or modify the exclusionary language must be preapproved by AIG Compliance.

If underwriting submissions or other communications suggest a misunderstanding by the broker or customer that AIG is extending coverage for sanctioned country operations, residents, or property, underwriters should correct that misunderstanding. Endorsements, schedules, tax forms and other policy-related documents should not refer to sanctioned countries in a way that could erroneously suggest coverage that the sanctions exclusionary language would exclude.

Even in cases where an AIG insurance policy has no sanctions exclusion, AIG will not pay any claim if it is unlawful to do so pursuant to U.S. Sanctions laws.

Escalation

Any potential sanctions issue must be immediately reported to the AIG Program Manager for handling. No business can be bound and no transaction can proceed without AIG Compliance approval.

Blocking and Reporting Property

Any property (including funds) which may be connected to a Sanctioned Party must be brought immediately to the attention of the AIG Program Manager so that arrangements can be made to block and report the property as required by U.S. law.

All records relating to property blocked pursuant to U.S. economic sanctions measures must be maintained for five (5) years after the property is unblocked. Property may only be unblocked with the consent of AIG Compliance.

The OFAC regulations are published in the Code of Federal Regulations, 31 CFR part 500. FAQs and a consolidated List of Specially Designated Nationals can be found on the OFAC website: http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

AIG's Economic Sanctions Policy may be accessed at the aigprograms.net website. Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

XVI. ANTI-MONEY LAUNDERING

Money laundering is any movement of criminal proceeds to disguise their origin and make them appear legitimate. In addition, money laundering is the term sometimes associated with financing activities carried out by legitimate business entities, charities, and individuals for the purpose of financing terrorist activities. One example of how money laundering can be accomplished through a property and casualty insurance company is when a purchaser of an insurance product pays funds to the insurance company with the expectation that the insurance company will return a substantial portion of such funds to the purchaser or the purchaser's designee at some future point in time.

Program Administrators are required to comply with the AIG Global Anti-Money Laundering Policy and are expected to promptly report to AIG any potentially suspicious activity connected to AIG customers or policies. Further, all Program Administrators must have written Anti-Money Laundering procedures designed to comply with any applicable Anti-Money Laundering laws.

Anti-Money Laundering Program Controls – Red Flag / Suspicious Activity Monitoring

Below is a list of some 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.

Underwriting Red Flags:

1. Customer is hesitant, provides minimal or seemingly false information, or delays, refuses, or appears reluctant to provide required information when requested.
2. Customer acting as agent for another will not disclose the identity of the principal.
3. Customer voluntarily requests early cancellation, especially at a significant cost, 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
4. Customer requests insurance that is not consistent with its needs and/or outside the its normal pattern of business.
5. Customer 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.
6. Customer shows little or no concern for the value or benefits of the insurance product, but shows much concern about early termination features.
7. Customer requests coverage for a business or high value personal asset, yet cannot, or will not, supply sufficient information about the business and the need for coverage.

Claims Red Flags:

1. 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.
2. Claimant requests the claim be paid in a different country or in a different currency from the premium.
3. Claim circumstances do not make sense, given the nature of the customer's business.

Collections Red Flags:

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

Program Administrator staff must be made aware of these indicators and, if suspicious activity is identified, investigate the facts. If any concern remains after investigation, the Program Administrator must the AIG Program Manager immediately. In the event that suspicious activity has been identified, under no circumstance may a customer be told that the customer is or was the subject of an internal investigation.

AIG's Anti-Money Laundering Policy may be accessed at the aigprograms.net website. Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

XVII. ANTI-CORRUPTION

AIG has anti-corruption policies prohibiting employees from offering or giving items of value directly or indirectly to a Government Official to obtain an improper business advantage. Examples of items of value are gifts, entertainment, payments, loans, trips, discounts and employment opportunities. A Government Official includes not only actual government members and agencies, but also employees of the following, as well as their family members:

- State owned entities*
- Public international organizations (e.g., the United Nations)
- Political parties and party officials
- Candidates for political office
- Members of royal families

*****_Some examples of state owned entities:_
  - Pension funds
  - State-run utilities
  - Public hospitals
  - Sovereign wealth funds

In performing their responsibilities, AIG's Program Administrators are expected to comply with all applicable anti-corruption laws and to maintain procedures designed to ensure the compliance of their directors, officers, employees and agents.

Program Administrators must not offer or provide to Government Officials on AIG's behalf payments, gifts, entertainment, travel training, or charitable or political contributions, or any other item of value without first obtaining the express permission of AIG. Nor shall such offers or gifts be given to persons with the knowledge that the benefit will be shared with Government Officials for the same purpose.

It is vital that AIG be aware of those who are acting on its behalf. Program Administrators must not hire or contract with other parties to assist in obtaining or retaining business for, or on behalf of, AIG without first obtaining AIG's express permission.

Program Administrators must not offer employment to Government Officials (including their family members) without written AIG approval, and must seek written AIG approval before permitting their directors, officers, employees or agents to become Government Officials during the term of the Program Administrator's agreement with AIG.

Program Administrators must maintain books and records which accurately reflect its business conducted in connection with or on behalf of AIG, and establish and maintain adequate internal accounting controls to ensure that AIG's anti-corruption objectives are being met.

AIG's Anti-Corruption Policy may be accessed at the aigprograms.net website. Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

XVIII. ANTITRUST

Antitrust laws are designed to prevent anticompetitive business practices. The primary antitrust law affecting AIG U.S. operations is the federal Sherman Act. Most states have also enacted antitrust laws. Federal and state antitrust laws generally prohibit agreements among competitors to fix prices, rig bids, allocate markets, boycott customers or suppliers, or engage in other anticompetitive activity that deprives customers of the benefits of vigorous competition. Sherman Act violations are prosecuted by the United States Department of Justice and are usually punished as criminal felonies. Individuals are subject to heavy fines and jail time, while corporations are subject to even heavier fines. Violations or allegations of violations of the antitrust laws can also lead to significant civil litigation, including class actions, and cause significant reputational harm to businesses and individuals. In civil antitrust suits brought by competitors or consumers, plaintiffs can recover treble damage awards plus the costs of bringing the suit, including attorneys' fees.

Price fixing is an agreement among competitors to raise, fix or otherwise maintain the price at which their goods and services are sold. The agreement need not address price directly to be illegal; an agreement on price related terms, such as payment terms, terms of sale, or various credits, are also illegal. Bid rigging involves competitors agreeing in advance on whose bid will be lowest in a competitive bid process. Boycotts are agreements among competitors not to deal with a particular (or particular class of) customer or supplier. Market allocation is an agreement pursuant to which competitors divide markets among themselves, whether by territory, type of customer or other criteria.

Except as may be required by law, companies must establish their own rates, prices, product offerings, and other terms and conditions of sale. Exchanges of information with competitors related to pricing must not take place. Obtaining pricing information from public sources, however, such as rate filings with regulators or the Internet is not prohibited. Participating in joint venture type arrangements, such as industry underwriting pools, may require exchanges of pricing information, but such exchanges should be limited to those relating to the joint venture's specific needs. Conversations with reinsurers may also require discussion of an insurance company's pricing.

Meetings with competitors should also be carefully structured to avoid discussions of improper subjects. Attendance of a neutral third party or assigned legal counsel will allow verification that discussion topics were proper. Discussions with competitors, whether in a formal meeting or an informal conversation, should avoid all discussion of rates, premiums, or methods of determining rates or premiums. More general discussions of market conditions and factors affecting business will generally not raise antitrust concerns and are permissible. In the event that the discussion in a meeting or telephone conference with a competitor or competitors departs from the agenda and turns to discussion of prices, premiums or other financial terms and conditions, or allocation of customers or territories or bids, the Program Administrator must leave the meeting, making clear to meeting participants contemporaneously and make sure the other participants take note that he or she has left and the reason for leaving, and may not discuss or reach any agreement or understanding on these inappropriate topics.

Tying arrangements, or requiring a customer to purchase an unwanted product (or a wanted product at a noncompetitive price) as a condition of purchasing a desired product, may also be unlawful. The determining factor is whether the company has a dominant presence in the market for the desired product sufficient to force the customer into the purchase of the other product. With respect to business conducted on behalf of AIG, Program Administrators must not make any determination concerning whether an antitrust issue exits. Such matters should be referred to your Program Manager, who will consult the AIG Legal Department or AIG Compliance Department as needed.

Proof of violations of the antitrust laws can be made by either direct or circumstantial evidence and involves discovery of correspondence, memoranda, personal and company files, and e-mail messages by law enforcement agencies. Careless statements may convey an impression of illegal action even when none has occurred. Communication with others should be conducted in an appropriate and professional manner.

AIG's Antitrust Policy may be accessed at the aigprograms.net website. Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

XIX. PRIVACY

The purpose of the AIG Global Information Handling Policy is to protect information about our Employees, customers and other individuals against unauthorized access or disclosure, maintain the accuracy of such information, and protect the confidentiality of non-public business information of AIG and other Third Parties with whom we do business. The proper handling of AIG information must be an important part of our business culture to ensure compliance with applicable legal obligations.

A. Definitions

1. **AIG Company Information**
   AIG Company Information includes "Firm Confidential," "Customer/Employee Confidential," and "Restricted" information.

2. **Customer/Employee Confidential information**
   Non-public information and information subject to legal protection about, or belonging to, our customers and customers of our business partners, other third parties with whom we do business, and AIG Personnel. Customer/Employee Confidential information can include Personal Information or Sensitive Personal Information (defined below) about an individual that is handled by, or under the control of, an AIG Entity (whether or not such Personal Information is publicly available from other sources external to AIG).

   a. Personal Information
   Personal Information includes information that identifies an individual, such as name, address, phone number and other Sensitive Personal Information.

   b. Sensitive Personal Information
   Sensitive Personal Information includes an individual's name in combination with their Social Security Number, Taxpayer Identification, passport number, driver's license number or other government issued identification number, financial account number, medical or health information, background check information (including criminal records), race, religion, ethnicity, marital status, or sexual orientation.

3. **Firm Confidential Information**
   Firm Confidential Information is information that is sensitive, non-public business information of the Company and its affiliates. Firm Confidential Information includes confidential business information such as: underwriting standards; pricing information; commission structures; terms and conditions of agency contracts; advertising materials that have not yet been approved or released to the public; non-public financial data about the Company; and selling know-how, that is, techniques, methods or concepts that have been created by the Company and are not generally known to the public.

4. **Restricted Information**
   This classification applies to non-public business information that is not as sensitive as Firm Confidential Information (as defined above), but which should still not be disclosed outside of the Company, as it is intended for internal use only. Examples may include general internal correspondence, including memoranda and emails, or marketing plans or

techniques, provided that they do not require the level of secrecy applied to Firm Confidential Information.

5. **Publicly Accessible Information**
   This classification applies to information that has been explicitly approved by AIG Entities for release to the public. Examples include public facing websites, product and service brochures, advertisements, public recruitment announcements, and press releases. By its nature, this information is not intended to be confidential.

B. Policy Requirements - All Information

Access to AIG Company Information should be limited to Program Administrators and their employees or associates who need to know the information in order to carry out their job functions or to provide timely and appropriate customer service. Such persons should be required to be familiar with and abide by the Company's privacy policies and requirements set forth herein.

Both during and after a Program Administrator's affiliation with the Company, a Program Administrator is prohibited, under the terms of its contract with the Company, from directly or indirectly divulging, publishing, communicating or making available to any person, corporation, governmental agency, or other entity, or using for their own or any other person's or entity's purposes or benefit, AIG Company Information (except with the written permission of the AIG Legal Department or as ordered by a court of competent jurisdiction or other regulatory authorities). If the Program Administrator is requested to provide AIG Company Information, including in connection with a legal or regulatory proceeding, contact the AIG Legal Department immediately.

While a Program Administrator is associated with the Company, all AIG Company Information compiled, received, held or used by them in connection with the business of the Company shall remain the Company's property and shall be destroyed or returned by them to the Company upon the termination of their association with the Company or at any earlier time requested by the Company, in accordance with the terms of the Program Administration agreement.
Program Administrators will be expected at all times, including after their relationship with the Company ends, to follow procedures for handling and storing AIG Company Information that are reasonably designed to prevent unauthorized access or use of the information.

C. Policy Requirements - Personal Information

1. Collection

Providing insurance products and associated services involves collecting customer personal, financial or health information that may not be publicly known. The Company and Program, Administrators collect information to underwrite insurance products, provide customer service and fulfill legal and regulatory requirements. Regardless of how or why the information is collected or in what form, the Company and Program Administrators are required by state and federal law and Company policies to protect and maintain the confidentiality of such information from unauthorized or improper disclosure.

Any Personal Information a Program Administrator collects or that was previously collected from an individual on the Company's behalf is subject to its privacy policies and privacy laws. These policies and laws also apply to any list or summary that is created from the Personal Information that was collected on the Company's behalf. For example, a Program Administrator -created list that contains the names and addresses of customers or prospective customers is Personal Information.

Program Administrators should only collect that Personal Information that is needed or sufficient to provide a product or service, or otherwise operate their business.

During any interaction with an individual, the Program Administrator may be working on behalf of the Company, a third party or parties (i.e., companies or individuals not affiliated with the Company), individual or on their own behalf. "Affiliate" or "affiliated" means any company that controls, is controlled by or is under common control with another company.

A Program Administrator is collecting Personal Information on the Company's behalf if they are using that information in connection with the authority that they have been given pursuant to the Program Administration agreement. Furthermore, a Program Administrator may be acting on the Company's behalf in collecting Personal Information -no matter how it is recorded- if the Producer represents to the individual that the Personal Information will be used to consider or obtain Company products or services or if the Program Administrator intends to use the Personal Information for that purpose.

There is no prohibition against Program Administrators collecting Personal Information on their own behalf, subject to any limitations to the contrary in the Program Administrator agreement. However, if a Program Administrator wants to collect or use Personal Information on their own behalf, they will need to comply with applicable privacy laws. This may require, among other things, that the Program Administrator prepare their own privacy notice for their current and prospective customers. They will also need to distribute that notice as the law requires and/or prepare and maintain their own customer consent or authorization forms.

2. Privacy Notice

Once an individual that is a consumer establishes a relationship with the Company- by purchasing insurance products or services for personal family or household use - the Company provides that individual a legally required Privacy Notice.

The Privacy Notice describes the types of Personal Information collected on the Company's behalf, how that information will be used and how the Company protects Personal Information. To supplement distribution of the Privacy Notice, Program Administrators may give the Privacy Notice to customers or prospective customers when requested or if the Producer deems it appropriate.

If the Program Administrator collects Personal Information on the Company's behalf or receives Personal Information from the Company, they are covered by the Company's

Privacy Notice and must comply with the Company's privacy policies. However, the Company's Privacy Notice will not satisfy the notice requirement, if any, for those situations in which the Program Administrator collects Personal Information on their own behalf or on behalf of a third party.

3. Disclosure of Personal Information Collected on the Company's Behalf

Limit the sharing of Personal Information to that necessary in connection with legitimate business activities. The following outlines the scope of a Program Administrator's authority to disclose Personal Information gathered on the Company's behalf or provided to the Program Administrator by the Company. These disclosure limitations also prohibit Program Administrators from using Personal Information collected on the Company's behalf when acting on their own behalf or on behalf of a third party. These prohibitions apply even after the Program Administrator's relationship with the Company ends.

The Program Administrator may only disclose Personal Information to the Company and the service providers the Company specifically designates, provided disclosure is necessary and appropriate, for any one of the following purposes:

a. To assist with underwriting a Company product or service;
b. To assist with placing or issuing a Company policy or service;
c. To effect, administer or enforce a transaction with the Company that the individual requested or authorized;
d. To service or process a Company product or service that the individual requested or authorized;
e. To assist the Company with claims administration or claims adjustment;
f. To assist the Company with detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; or
g. To respond to lawfully served subpoenas or production requests from regulatory or judicial authorities after contacting Legal and providing a copy of the subpoena or request to Legal.

4. Marketing

When an individual's Personal Information will be shared with affiliated or unaffiliated third parties for marketing purposes (where permitted by applicable law), the individual should be provided an opportunity to limit the sharing of such Personal Information (i.e., opt out) as required by applicable law, or the individual's consent should be obtained prior to the sharing of such Personal Information (i.e., opt in), as required by applicable law.

XX. DATA SECURITY

All Program Administrators must comply with AIG's Data Security Standards, which are set forth below:

A. Definitions.

1. "Confidential Information" means any information, except for Excluded Information, provided or made available by or on behalf of AIG in connection herewith (including, without limitation, (i) third party materials or information used by AIG, and (ii) any materials or other information provided during an inspection of AIG's books and records), together with all analyses, compilations, data, studies or other documents or records that contain, otherwise reflect or are generated or derived from such materials or other information. For the avoidance of doubt, Personal Information is Confidential Information.

2. "Excluded Information" means any information, other than Personal Information and data pertaining to the information security of AIG, that:

   a) is properly in the possession of the Program Administrator on a non-confidential basis prior to the Program Administrator receiving the same information from AIG;

   b) is or becomes available to the general public from another source without breach of any contractual, legal, fiduciary or other obligation with or to AIG or a third party that is known or should have been known to the Program Administrator;

   c) is disclosed to the Program Administrator on a non-confidential basis by another source without breach of any contractual, legal, fiduciary or other obligation with or to AIG or a third party that is known or should have been known to the Program Administrator; or

   d) is independently developed by the Program Administrator without use of or reliance upon the Confidential Information.

   Information obtained, derived or available from sources known to include illicit data, such as the "dark web," do not meet the requirements of the exceptions in (a)-(d) above.

3. "Information Systems" means any computer, computer network, computer application, imaging device, storage device or media, mobile computing device, or any other information technology that contains Confidential Information.

4. "Personal Information" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly with a particular individual or household accessed by the Program Administrator in connection with the performance of its obligations under the Agreement, including, but

not limited to, (a) an individual's name, address, e-mail address, IP address, telephone number, (b) the fact that an individual has a relationship with AIG and/or its parent, affiliated or subsidiary companies, (c) an individual's account information, and (d) any other information protected by Data Privacy Laws.

5. "Privacy and Security Laws" mean all laws and regulations, as amended or re-enacted from time to time, applicable to the Program Administrator or AIG, pertaining to the security of Confidential Information and Information Systems ("Security Laws") and the protection or privacy of Personal Information ("Data Privacy Laws").

6. "Representatives" means any of the Program Administrator's affiliates, consultants, third party program administrators, attorneys, actuaries and auditors that assist the Program Administrator in the Services Purpose (defined below).

7. "Security Incident" means any actual or reasonably suspected: (i) unauthorized use of, or unauthorized access to, Information Systems, (ii) damage to, or inability to access, Confidential Information or Information Systems due to a malicious use, attack or exploit of such Confidential Information or Information Systems, (iii) unauthorized acquisition, alteration, disclosure, theft, or loss of or access to Confidential Information, (iv) unauthorized use of Confidential Information for purposes of actual, reasonably suspected, or attempted theft, fraud, identity theft or other misuse, (v) transmission of malicious code to AIG's Information Systems arising from, in whole or part, an act, error, or omission of the Program Administrator, or its Representatives, or (vi) any other cybersecurity event or Personal Information breach as defined in Privacy and Security Laws.

B. Permitted Use. The Program Administrator and its Representatives shall access, use, transmit, store, and otherwise process the Confidential Information and Information Systems only to the extent necessary for the Program Administrator to exercise its rights under this Agreement and perform its obligations under this Agreement and for internal administration, risk management, regulatory compliance and accounting purposes related thereto (the "Services Purpose"). AIG shall be permitted to access, use, transmit, store, disclose and otherwise process confidential information provided by the Program Administrator only as necessary for AIG to exercise its rights under this Agreement and perform its obligations under this Agreement and for internal administration, risk management, regulatory compliance and accounting purposes related thereto, provided that such information is clearly identified by the Program Administrator in writing as confidential, proprietary or a similar designation. The terms and conditions of the Agreement are the confidential information of both parties. The Program Administrator shall ensure that its personnel and those of its Representatives with access to Personal Information are subject to a contractual duty of confidence to hold the Personal Information in strict confidence to at least the standard required herein.

C. Compliance with Laws. The Program Administrator will comply with the Privacy and Security Laws and shall cooperate with AIG's efforts to comply with such laws, including by taking such steps as are requested by AIG to assist AIG in meeting its obligations under

Privacy and Security Laws with respect to security, security breach notification, data protection or privacy impact assessments, and consultation with regulators. Except as prohibited by law, the Program Administrator shall promptly advise AIG in writing if it receives or learns of any complaint or allegation indicating a violation of Privacy and Security Laws regarding the Confidential Information and shall investigate and resolve the matter, including, but not limited to, preparing the response to such complaint or allegation for AIG's approval, implementing a remedy (if applicable), and/or cooperating with AIG in the conduct of and defending against any claim, court or regulatory proceedings.

D. Third Party Providers. Except as permitted in Paragraph F., the Program Administrator must obtain AIG's prior written approval before the Program Administrator allows any third party (including Representatives) to access or use Information Systems or access, use, transmit, store, or otherwise process the Confidential Information. Prior to any such access, use, transmission, storage or processing, the third party recipients, including the Program Administrator's Representatives, must have a written agreement with the Program Administrator that includes terms at least as protective as set out in herein and on an ongoing basis, the Program Administrator must oversee and review such third parties for privacy, confidentiality, and information security risks, controls, and compliance. The Program Administrator and its Representatives shall not disclose, transfer or otherwise make available Confidential Information to any third party in exchange for monetary or other valuable consideration. The Program Administrator shall be responsible for any acts and omissions by any of its Representatives or other parties to which it discloses Confidential Information or provides access to the Information Systems.

E. Return/Destruction of Confidential Information. The Program Administrator shall, and shall cause its Representatives to, promptly return, delete or destroy (at AIG's option) the Confidential Information when no longer needed for the Services Purpose, on termination of the Agreement or when requested by AIG, whichever occurs first. The Program Administrator will certify that it has securely shredded paper copies and permanently deleted or destroyed electronic copies rendering it no longer usable, readable, decipherable or retrievable. In the event the Program Administrator is unable to return or delete the Confidential Information for reasons permitted by Privacy and Security Laws, the Program Administrator will (i) promptly inform AIG of the reason(s) for its refusal of the return or deletion request, (ii) continue to abide by the privacy, confidentiality, and security obligations hereunder of such Confidential Information, and (iii) return or delete (as applicable) the Confidential Information promptly after the reason(s) for refusal has expired.

F. Required Governmental Disclosures. Nothing herein shall prohibit the Program Administrator from disclosing this Agreement and/or any Confidential Information, or providing access to any Information Systems, to the extent required to comply with a valid court order or other directive from a government authority having jurisdiction over either of the parties (each a "Governmental Directive"). In the event the Program Administrator is made aware of an effort by any entity to obtain a Governmental Directive requiring disclosure of or access to any Confidential Information or Information Systems, the Program Administrator shall notify AIG immediately, to the extent not prohibited by law, and shall cooperate with AIG's efforts, which shall be at AIG's expense, to challenge or otherwise

respond to the Governmental Directive. With respect to any disclosure made pursuant to this Paragraph, the Program Administrator (or any of its Representatives) agrees to furnish only that portion of the Confidential Information that it reasonably determines, in consultation with its counsel, is necessary under applicable law.

G. Assessments. AIG may perform or have a third party (including a regulator) perform, reasonable privacy and/or security audits, investigations or assessments of the Program Administrator upon reasonable notice, and the Program Administrator shall timely provide all reasonably requested reports, information or access in connection therewith. The Program Administrator represents and warrants that the information provided by or on its behalf in response to AIG's privacy and/or security audits, investigations or assessments is complete, truthful, and accurate, and that the Program Administrator shall have and/or comply with the measures and controls described in any such audits, investigations or assessments.

H. Comprehensive Security Program. The Program Administrator shall maintain a comprehensive information security program designed to protect the confidentiality, integrity and availability of Confidential Information and Information Systems, and to protect all Confidential Information from unauthorized use, alteration, access, acquisition, processing, disclosure or loss. The information security program shall, at a minimum, comply with the requirements of Privacy and Security Laws and, in particular, shall include: (i) written policies and procedures, which shall be periodically assessed and revised to address changes in risks and the effectiveness of controls; and (ii) technical, administrative, physical, organizational and operational measures and controls to ensure a level of security appropriate to the information security risk (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons) and consistent with industry best practices as they evolve over time, including encryption of Confidential Information at rest and in transit, controls to limit unauthorized access to Information Systems and Confidential Information, the use of multi-factor authentication when accessing any Information Systems from outside AIG's network, and periodic vulnerability scanning and penetration testing.

I. Security Incident. The Program Administrator shall promptly provide written notice to AIG (and in no event later than two (2) days after becoming aware) of a Security Incident and shall cooperate with AIG to investigate and respond to any such Security Incident. The Program Administrator shall: (i) take all reasonable measures to contain, mitigate and remedy the Security Incident, wherever possible and without delay; (ii) provide AIG with information regarding the investigation and remediation of the Security Incident, unless restricted by law; (iii) not make any notification, announcement or publish or otherwise authorize any broadcast of any notice or information about a Security Incident that identifies AIG (a "Breach Notice") without the prior written consent of and prior written approval by AIG of the content, media and timing of the Breach Notice (if any), unless required to do so by law or court order; and (iv) even where required to do so by law or court order, make all reasonable efforts to coordinate with AIG prior to providing any Breach Notice. To the extent arising from the Program Administrator's failure to comply with any requirements herein, at the request of AIG, the Program Administrator shall reimburse AIG for the

following expenses incurred by AIG with respect to any Security Incident: (i) costs to notify AIG's customers, clients and/or employees, law-enforcement agencies, the media, regulators, brokers, agents, and business partners, or other third parties, (ii) costs to investigate, assess, or remediate any Security Incident (including attorneys' and legal fees and costs), (iii) public relations consultant expenses, (iv) expenses to retain a call center and other relevant communication facilities to respond to inquiries regarding any Security Incident, (v) expenses pertaining to responding to government authorities, law-enforcement agencies, or regulators' investigations, (vi) fines or penalties imposed by a regulator or other governmental agency; and (vii) where the Security Incident involves data elements that could lead to identity theft, credit monitoring or other commercially-reasonable identity theft mitigation service for the affected individuals for up to one year or such longer period as required by law or a government regulator. The Program Administrator's obligations in this Paragraph are not subject to or limited by any consequential or indirect damage disclaimer provision, limitation of liability section, or other liability exclusions or waivers elsewhere in the Agreement.

J. Individual Rights. The Program Administrator will promptly inform AIG in writing of any requests with respect to Personal Information. Except as prohibited by law, the Program Administrator shall also promptly advise AIG in writing if it receives or learns of any request from one or more individuals seeking to correct or delete Personal Information. The Program Administrator shall, at AIG's request and in accordance with AIG's instructions, assist AIG in responding to, and complying with, all individual rights requests relating to the Personal Information exercised pursuant to Privacy and Security Laws, including by providing any requested information in a portable and, to the extent technically feasible, readily useable format that allows the individual to transmit the information to another entity without hindrance.

K. Processor Framework. The parties agree that, for the purposes of Privacy and Security Laws, the Program Administrator (to the extent it processes Personal Information pursuant to or in connection with this Agreement on behalf of AIG) processes Personal Information as a processor (as that term is defined in Privacy and Security Laws). A description of the Personal Information processing activities performed by the Program Administrator is located at Section 6, Section 8 and Section 14 of the Agreement. Without prejudice to the Program Administrator's other obligations set forth herein, the Program Administrator agrees to: (i) only process the Personal Information as expressly permitted by this Section (these being AIG's documented instructions) and otherwise in accordance with the written instructions given by AIG, unless the Program Administrator is subject to an obligation under applicable law to do otherwise, in which case the Program Administrator shall notify AIG in advance of that legal obligation (unless prohibited by that law on important grounds of public interest); and (ii) notify AIG immediately if, in the Program Administrator's opinion, an instruction from AIG breaches a requirement of Privacy and Security Laws.

L. Cross Border Transfer. The Program Administrator shall not (and shall procure that its Representatives shall not) disclose or transfer Personal Information internationally without the prior written consent of AIG. Where AIG consents to the Personal Information being disclosed or transferred internationally to or by the Program Administrator or its

Representatives, the Program Administrator shall, as reasonably requested by AIG, execute an appropriate contract to comply with Privacy and Security Laws, such as standard model contract clauses approved by the governing body with jurisdiction over AIG or AIG's International Data Processing and Transfer Agreement.

M. Equitable Relief. The Program Administrator hereby acknowledges and agrees that monetary damages may be both incalculable and an insufficient remedy for any breach hereof by the Program Administrator or its Representatives and that any such breach may cause AIG irreparable harm. Accordingly, AIG shall be entitled to seek equitable relief, including, without limitation, injunctive relief and specific performance, in the event of any breach of the provisions set forth herein by the Program Administrator or its Representatives, in addition to all other remedies available at law or in equity.

N. Third Party Beneficiary. With respect to Confidential Information or Information Systems of AIG's Affiliates, such Affiliates are intended third party beneficiaries of your Program Administrator for the purposes of the data security requirements set forth herein and will be entitled to enforce the provisions hereof as if each was a signatory to the Agreement, and for these purposes references to AIG in this Section shall be deemed to include references to the relevant Affiliate. AIG and the Program Administrator may, in accordance with this Agreement, vary, rescind or terminate this Agreement (whatever the nature of such variation, rescission or termination) without seeking the consent of any third party on whom this Paragraph confers rights.

XXI. THIRD PARTY CODE OF CONDUCT

AIG is committed to conducting its business in accordance with the highest ethical standards and in full compliance with all applicable laws and regulations in the United States and in other jurisdictions in which AIG operates or does business. As part of that commitment, AIG expects all companies and individuals with whom it does business to do the same. AIG counts on each of its Program Administrators acting on AIG's behalf to adhere to the same core values and principles as AIG. To that end, all Program Administrators are required to comply with the AIG Third Party Code of Conduct, which summarizes AIG's expectations for all Third Parties engaged by AIG.

AIG's Third Party Code of Conduct may be accessed at the aigprograms.net website. Questions regarding this policy should be directed to the AIG Program Manager responsible for the program. The AIG Program Manager will coordinate with the AIG Legal Department as necessary.

APPENDIX A

AIG INSURANCE COMPANIES

ADMITTED COMPANIES

AIG Assurance Company[3]
AIG Property Casualty Company[4]
American Home Assurance Company
Commerce and Industry Insurance Company
Granite State Insurance Company
Illinois National Insurance Co.
National Union Fire Insurance Company of Pittsburgh, Pa.
New Hampshire Insurance Company
The Insurance Company of the State of Pennsylvania

NON-ADMITTED COMPANIES

AIG Specialty Insurance Company[5]
Lexington Insurance Company

[3] Formerly known as Chartis Casualty Company
[4] Formerly known as Chartis Property Casualty Company
[5] Formerly known as Chartis Specialty Insurance Company