AIG DOMESTIC BROKERAGE GROUP

PROGRAM ADMINISTRATOR LEGAL COMPLIANCE MANUAL

June 2006

TABLE OF CONTENTS

I. INTRODUCTION

The reputation and success of the insurance companies writing property and casualty, workers' compensation and accident and health insurance, within the AIG Domestic Brokerage Group (hereinafter referred to as the "Company" and listed in Appendix A), depends on complying with all relevant state and federal laws and regulations**.** Thus, any action 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 handling policies on behalf of the Company.

To understand the Program Administrator's role in the Company's business, each Program Administrator must be aware of the legal and regulatory environment in which it operates. Each state has tailored its insurance laws and regulations to best serve its own public policy. Accordingly, the laws and regulations relating to any given area of insurance may differ from state to state.

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. Therefore, as an independent contractor 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 Agreement is the contract that sets forth the relationship between the Company and the Program Administrator and the Company's expectations.[1] 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 by any state insurance department.

Attorneys in AIG Domestic Brokerage Group Legal Services ("DBG Legal Services") provide advice to Domestic Brokerage Group business units on legal and regulatory issues affecting their businesses. DBG Legal Services assists AIG Domestic Brokerage Group entities 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 DBG Manager responsible for the program. The DBG Manager will coordinate a response with DBG Legal Services.

This 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 compliance issues and requirements established by the Company. It is recommended that each Program Administrator establish its own compliance program.

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

II. REGULATORY COMPLIANCE

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; and adherence to filed and approved forms and rates. Program Administrators have an obligation to keep abreast of and follow these rules and regulations.

Cancellation or non-renewal of the Companies' policies must be effected in compliance with the cancellation and non-renewal procedures set forth in each insurance policy and any applicable legal or regulatory requirement.

When a program is cancelled or withdrawn from a territory, additional requirements governing "block cancellations" or "blanket or mass withdrawals" may apply. Such block cancellation/withdrawal requirements may include specific regulatory and policyholder notice and approval requirements.

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, and age or disability status. Failure to comply with procedural cancellation and non-renewal requirements may render the cancellation and non-renewal ineffective, and subject the Company to regulatory sanctions.

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

Failure to comply with the applicable legal and regulatory state filing requirements may affect the Company's ability to enforce policy terms or collect premiums and may subject the Company to regulatory fines and other sanctions.

Questions regarding regulatory compliance should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

III. PRODUCER LICENSING, APPOINTMENTS AND COUNTERSIGNATURE

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 of business hold appropriate licenses.

Additionally, states have producer appointment requirements that must be complied with. All Program Administrators must respond promptly to requests for copies of licenses and cooperate with completion of background checks and all other activities surrounding the appointment process.

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, may be responsible for any damages, penalties, fines and liabilities incurred as a result of any violation.

The Program Administrator shall immediately notify the Company of any lapses, cancellations, suspension or termination of any license necessary to fulfill its duties under its Program Administrator Agreement.

The Program Administrator is solely responsible for ensuring that all business is properly countersigned and all necessary countersignature expenses are paid in those states with countersignature requirements.

Questions regarding countersignature or producer licensing should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

IV. ADVERTISING

Insurance advertising is highly regulated and subject to scrutiny under 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 (a) to create public interest in insurance, an insurer, or an insurance product or (b) to induce the public to purchase, increase, modify, reinstate, borrow on, surrender, replace or retain an insurance policy. Advertising includes printed, published and audiovisual material, 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 also regulated by federal and state statutes and regulations relating to advertising.

All materials that in any way could be considered an advertisement or part of an advertisement that names or references American International Group, Inc. (AIG) or any AIG member company in any way, including logos, trademarks, tradenames, service marks or financial materials, must be approved by DBG Legal Services in writing prior to use.

Questions regarding advertising should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

V. CONFIDENTIALITY & PRIVACY

The Company has established policies and procedures to protect the security and confidentiality of customer information and requires Program Administrators to do the same. Within the Program Administrator's organization, such information should be shared only on a need-to-know basis in furtherance of the business of the Company and the Program Administrator.

A. STATE REGULATIONS

Statutory and regulatory requirements mandate that certain types of information held by commercial entities must be kept confidential. These types of information include:

(1) Personal financial information;
(2) Personal health information; and
(3) Proprietary information of commercial insureds.

Many states have laws and/or regulations that establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions. Generally, these laws and regulations provide that the following types of individually identifiable information must be kept confidential:

(1) Information provided by natural persons who are the subject of information collected, received or maintained in connection with insurance transactions involving applications, policies, contracts or certificates of insurance;
(2) Information that relates to a claim for health insurance benefits;
(3) Information from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristics; and
(4) Public information that is altered for a business purpose. For example, if a Program Administrator retrieves individuals' telephone numbers from the phone book (the content of which is public information) to augment its customer database, the telephone numbers become nonpublic information once integrated into the customer database.

Except for information that may be considered "public information", the failure to keep confidential any such information may result in potential regulatory and civil liability for both direct and consequential damages.

B. FEDERAL REGULATIONS

(1) Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act ("GLBA"), enacted in 1999, establishes a comprehensive regulatory framework governing the privacy practices and procedures of financial institutions. The law requires financial institutions to develop and disseminate notices of their privacy policies and contains several restrictions on the disclosure of a consumer's personal financial information. In addition, regulations implementing the Act are determined by "functional regulators" (*e.g.*, Securities Exchange

Commission for securities dealers and brokers and the Office of Thrift Supervision for thrifts). Regulations for the insurance industry may be written by each individual state insurance authority. States are free to adopt more stringent consumer protections than those provided under GLBA.

In general, GLBA requires:

a. Initial and annual disclosure of Company privacy practices to all customers. (Customers are consumers who have on ongoing relationship with a financial institution. Consumers are individuals obtaining financial products or services to be used primarily for personal, household, or family purposes.);
b. Disclosure to consumers of the Company's intent to share nonpublic personal financial information about consumers with nonaffiliated third parties outside the normal course of business;
c. Providing consumers an opportunity to opt-out of disclosure of nonpublic personal financial information to nonaffiliated third parties;
d. Limiting the reuse of nonpublic personal information received from another financial institution to the standards contained in the privacy policy of the financial institution providing the information;
e. Monitoring and ensuring vendor compliance with the insurer's privacy policy;
f. Education of employees, agents and others regarding privacy duties; and
g. A written plan to protect the security, integrity, and confidentiality of customer financial information.

(2) Health Insurance Portability and Accountability Act

The purpose of the privacy regulations issued by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act ("HIPAA") is to set guidelines for the use and disclosure of an individual's protected health information ("PHI"). Generally, HIPAA requires an authorization by the individual for disclosure of PHI by a covered entity for any reason other than payment, treatment or health care operations.

A covered entity is defined as: (i) a health plan, which is an individual or group health plan that provides or pays the cost of medical care; (ii) a health care clearinghouse, an entity that processes or facilitates the processing of health information; and (iii) a health care provider who transmits any health care information in electronic form.

PHI is defined as any individually identifiable health information transmitted or maintained by a covered entity.

Use and Disclosure of PHI by a Covered Entity:

a. All covered entities must obtain an individual's specific written authorization to use and disclose PHI for any reason other than treatment, payment or health care operations. If PHI is required to be disclosed by law or for public health purposes, the authorization requirement is waived.
b. If a covered entity discloses PHI to a "business associate", the covered entity is required to obtain an agreement from the business associate stating that it will protect PHI and handle it in accordance with the law. A business associate is defined as a person who performs a function or activity regulated under the HIPAA regulations on behalf of a covered entity but excludes a person who is part of a covered entity's workforce. A business associate may also be a covered entity.
c. When disclosing or requesting PHI for any reason other than treatment, a covered entity must make reasonable efforts to limit the PHI disclosed or requested to the minimum necessary to accomplish the intended purpose of use.

A covered entity may de-identify PHI by removing all personally identifiable items such as name, birth date, phone number, social security number, etc.

Administrative Requirements of a Covered Entity:

a. A covered entity must designate a privacy official who is responsible for implementing and developing the covered entity's privacy policies and procedures.
b. A covered entity must provide training on privacy rules to all members of its workforce who will have access to PHI.
c. A covered entity must put in place administrative, technical and physical safeguards to protect the privacy of PHI from accidental or intentional use or disclosure in violation of law and to protect against inadvertent disclosures to parties other than the intended recipients.
d. A covered entity must have a mechanism for receiving complaints from individuals regarding the covered entity's privacy practices.
e. A covered entity must have written disciplinary policies and procedures for members of its workforce who fail to comply with the entity's privacy practices.
f. A covered entity must notify individuals of how it may use and disclose PHI.

Individuals' Rights under HIPAA:

a. An individual has the right to restrict a covered entity's use and disclosure of PHI.

b. An individual has the right to inspect and make copies of his or her PHI but a covered entity may deny access for reasons specified under the regulations.
c. An individual has the right to amend PHI about the individual that is incorrect or inaccurate.
d. An individual has the right to receive an accounting for disclosures of PHI to any entity, including a business associate, for reasons other than payment, treatment or health care operations.

C. BREACH OF DATA SECURITY

Many states have enacted laws that require entities or persons in possession of certain information to provide notice to all individuals affected by data security breaches especially with respect to unencrypted data elements (e.g. social security numbers, driver's license numbers, account numbers plus personal identification numbers or passcodes and in some states medical information). There are strict notice requirements to be followed under these circumstances including the form, type, substance and timeliness of the notice. Program Administrators must immediately (1) notify the Company upon the breach or compromise of any of the foregoing types of information and (2) secure the data and information from any further unauthorized disclosure or release.

D. CANADIAN PRIVACY LAW

Program Administrators operating in Canada must also comply with Canadian privacy laws, regulations, rules and guidelines. Canada has two federal privacy laws, the Privacy Act and the Personal Information Protection and Electronic Documents Act. There are also provincial laws that must be observed.

The Canadian privacy laws seek to prevent unlawful or unauthorized disclosure of confidential and personal information. However, a significant concern involves cross-border data flow and disclosure of information pursuant to the U.S. Patriot Act. The U.S. Patriot Act enables U.S. authorities to access information of any foreign person if the information resides within its jurisdiction. The Canadian laws require that notice be provided to Canadian consumers and customers that their personal information may be subject to governmental disclosure in a foreign jurisdiction (i.e. the United States). In some instances, there are also restrictions and prohibitions to the flow of data outside of Canada and will be permitted only under certain narrow exceptions.

Canadian privacy legislation continues to develop and therefore Program Administrators must be keenly aware of upcoming changes to the law.

All Program Administrators must comply with the confidentiality and privacy laws in the states in which they transact business.

Questions regarding confidentiality and privacy should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

VI. 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 of 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 for the information 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. These laws and regulations also may affect the exchange of consumer credit information between related AIG Companies.

Questions regarding the use of consumer credit reports should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

VII. FRAUD

Fraud involving or affecting the Company is a serious threat to the Company's ability to do business.

Fraudulent activities may occur in virtually any aspect of the insurance business, and may occur through bribery, fictitious policies, fictitious claims on legitimate policies, or accounting and other record keeping irregularities. Fraudulent activities, including fraudulent claims, embezzlement or misappropriation of an insurer's property, are prohibited by law and may form the basis of both civil and criminal liability under both federal and state laws. The Company has implemented antifraud initiatives calculated to prevent and detect fraudulent insurance acts, and will refer suspected fraudulent activities to appropriate agencies, whether allegedly committed by persons inside or outside of the Company. The following types of activities may be indicative of insurance fraud:

(1) Applicant for insurance coverage understates or misrepresents pending litigation, number/classification of employees, commercial vehicles, *etc.*, or past claims history;
(2) Claimant overstates the value of property damaged or destroyed;
(3) Injured employee exaggerates the seriousness of an injury or refuses to provide previous medical history; and
(4) Claimant refuses to allow claims adjuster to inspect damaged property.

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 DBG Manager responsible for the program, who will in turn immediately contact DBG Legal Services. 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 DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

VIII. 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 subproducers to the DBG Manager responsible for the program, who will in turn immediately contact DBG Legal Services.

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 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 DBG Manager responsible for the program, who will in turn immediately contact DBG Legal Services.

Any person who intentionally withholds such information is in violation of the AIG Compliance Program.

IX. ANTITRUST

POLICY STATEMENT:

Federal antitrust laws are designed to prevent anticompetitive business practices. The primary federal antitrust law affecting your business with DBG is the 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. For each offense, individuals can be fined up to $1,000,000 and sentenced to up to ten years in federal prison, while corporations can be fined up to $100 million or the amount of the harm to consumers. 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. Your business practices as well as those of the DBG Companies are subject to these laws. Your actions may subject the DBG Companies to violations under these laws[2].

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 directed by specific statutes, companies must establish their own rates, prices, product offerings, and other terms and conditions of sale. Exchanges of information related to pricing with competitors should be avoided. 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. If an employee finds himself/herself in a discussion with a competitor, whether a formal meeting or an informal conversation, avoid all discussion of rates, premiums, or methods of determining rates or premiums. If a competitor brings up an improper discussion topic, interrupt him or her by stating that it is company policy not to discuss such topics with competitors. If the competitor persists, end the discussion, leaving the meeting if necessary.

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 the market power over, or a

[2] American Society of Mechanical Engineers, Inc. v. Hydrolevel Corporation, 456 U.S. 556, (1982)

dominant presence in, the market for the desired product sufficient to force the customer into the joint purchase.

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. Employees should protect themselves and the company by communicating with others both inside and outside the company in an appropriate and professional manner. Employees should avoid saying or writing anything that they would not be willing to repeat to a judge or jury or that they cannot adequately explain years after the events.

Program Administrators should address any questions about antitrust compliance to their legal counsel.

X. 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 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 the FDCPA and other relevant 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; and
(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.
(10) Commencing or causing to be commenced any lawsuit, arbitration or other adversary proceedings in any forum against any individual or corporate entities 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 DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

XI. GIFTS, BRIBES & POTENTIAL CONFLICTS OF INTEREST

The Company has established policies regarding gifts, bribes, compensation, payments, loans, entertainment, salvage, or preferential treatment, whether given or received, and any other circumstances that may result in an actual, potential or perceived conflict of interest. Program Administrators should also establish their own policies in order that they and their employees avoid all situations, behavior or relationships that might impair their ability to represent the Company's interests fairly and impartially.

Questions regarding this policy should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

XII. POLITICAL CONTRIBUTIONS

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

Questions regarding this policy should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

XIII. DOCUMENTS & RECORDS MANAGEMENT

State insurance laws and regulations require that the Company maintain different types of records for different periods of time. Failure to observe these requirements can result in regulatory sanctions, as well as civil liability and/or excessive litigation costs.

All Program Administrators are required to keep complete and accurate copies of all records of the business transacted by it for the Company as specified in the DBG Records Management Policy and as required by the Program Administrator's Agreement. The Company also expects that books, records, documents and other business records will be maintained in such an order that data is readily accessible and retrievable.

Company Records should be destroyed on a regular basis after the minimum applicable retention period set forth in the DBG Records Management Policy. However, if any Program Administrator or any of its employees knows or can reasonably foresee that a Company may be a party to litigation, a government investigation or a regulatory proceeding, the DBG Manager responsible for the program must be notified and no record that may be relevant to such litigation, investigation or proceeding may be destroyed. The DBG Manager will immediately notify DBG Legal Services.

Questions regarding document and records retention should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

XIV. UNLAWFUL DISCRIMINATION

The Company is committed to applying designated 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 race, color, religion, sex or national origin.

State statutes 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.

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 is not authorized the 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 DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

XV. U.S. ECONOMIC SANCTIONS AND TRADE EMBARGO COMPLIANCE

The Office of Foreign Asset Control ("OFAC") of the U.S. Department of Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, government entities, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. Accordingly, OFAC (1) enforces laws and regulations targeting certain countries against which the U.S. has imposed sanctions or trade embargoes and (2) has identified and named numerous foreign agents and front organizations, as well as terrorist and terrorist organizations as Specially Designated Nationals and Blocked Persons. The country sanctions and the Specially Designated Nationals and Blocked Persons list can be accessed through OFAC's website at http://www.ustreas.gov/offices/enforcement/ofac/. By law, U.S. underwriters, brokers, agents, primary insurers, and reinsurers are prohibited from engaging in transactions, including claim payments, (1) that violate country sanctions and trade embargoes or (2) with individuals or entities appearing on OFAC's Specially Designated Nationals and Blocked Persons list.

Adherence to OFAC administered rules and regulations is critical. OFAC has the authority to impose both civil and criminal penalties. Depending on the violation, criminal penalties can result in corporate fines of up to $1 million and 12 years imprisonment.

All Program Administrators are prohibited from conducting transactions that would violate such economic sanctions and trade embargoes. Prior to entering into any transaction, the Program Administrator must check to determine whether such transaction (1) violates any country sanctions or trade embargoes or (2) is with a person, entity or country appearing on OFAC's Specially Designated Nationals and Blocked Persons list. If a Program Administrator is transacting business with a targeted individual or entity, it must "freeze" the transaction. Freezing the transaction requires placing any monies attributable to the transaction in a blocked interest bearing account.

Upon discovery of a potential transaction or executed transaction with a targeted person, entity or country, the discovery must be reported immediately to the DBG Manager responsible for the program. The DBG Manager responsible for the program will notify DBG Legal Services and DBG Legal Services will determine whether the transaction needs to be reported to OFAC.

Questions regarding OFAC rules should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

XVI. MONEY LAUNDERING

"Money Laundering" is the process by which criminals conceal the nature or source of their illegal funds and disguise such funds by moving them through U.S. financial institutions to make them appear legitimate. Money laundering can be accomplished through a property and casualty insurance company 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. Primary examples are:

A. Transactions whereby an insurance company accepts collateral in connection with an insurance policy;

B. Policies that involve a commutation feature, i.e., the insurance company may be obligated to pay money back to the purchaser if losses are below a certain level; and

C. Policies being cancelled, followed by refunds of premium to the purchasers.

To prevent, detect and control money laundering, program administrators must **know their customers** – by obtaining proper identification and sufficient information about the customer and the customer's business and by conducting due diligence appropriate to the circumstances to be able to determine the customer's apparent legitimacy. Knowing the customer involves identifying "red flags" with respect to these **types of products**.

Red Flags might be:

Source of Funds

Is the money that will fund the purchase coming from a source other than a reputable financial institution or from a financial institution regulated by one of the countries or territories identified by (1) The Financial Crimes Enforcement Network of the U.S. Department of Treasury ("FinCEN") (see www.fincen.gov) or (2) The Office of Foreign Assets Control of the U.S. Department of Treasury ("OFAC")?

Geographic

Is the prospective purchaser a resident of or domiciled in any country or territory that has been identified by FinCEN as a high risk or non-cooperative country or against which OFAC has enforced economic and trade sanctions?

Suspect Circumstances

i. Does the prospective purchaser have unusual concern for secrecy, particularly with respect to his identity, type of business, assets or dealings, or have non-verifiable references or appear to be reluctant or refuse to provide financial information or information concerning financial relationships and business activities?

ii. Does the prospective purchaser exhibit a lack of concern for risks, commissions or other transaction costs?

iii. Does the prospective purchaser appear to operate as an agent for an undisclosed principal and be reluctant to provide information regarding such principal?

iv. Does the prospective purchaser have difficulty describing the nature of his business or exhibit a lack of general knowledge of his industry?

v. Does the prospective purchaser have a questionable background, including prior criminal convictions, or rely on unusual or suspect identification or business documents?

All Program Administrators must be alert to the implications of money laundering. The inadvertent participation in money laundering can be avoided by exercising due diligence and caution. All suspected cases of money laundering should be reported immediately to the DBG Manager responsible for the program, who will in turn immediately contact DBG Legal Services.

Questions about money laundering should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

XVII. *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 restricted hours.

On October 1, 2003, the FTC and FCC implemented new regulations regarding telemarketing. The federal government now requires any company that utilizes telephone marketing to verify its call-list against a *National Do Not Call Registry*. Over fifty million people have registered with the National Registry.

Program Administrators are required to follow the guidelines with 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. DBG 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.

Questions regarding this policy should be directed to the DBG Manager responsible for the program. Where legal counsel is required, the DBG Manager will coordinate a response with DBG Legal Services.

XVIII. BUSINESS REQUIREMENTS

A. INSURANCE

The Program Administrator must obtain and maintain all insurance coverage as stipulated in the Program Administrator Agreement. The Program Administrator must also provide the insurer with certificates of insurance which reflect the approved limits of liability, name the Insurer as an additional insured or loss payee, as appropriate, and provide that the Insurer will receive 30 days' written notice of any change, cancellation or other termination of such policies.

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

B. SUBCONTRACTING

The Program Administrator shall not subcontract services for the Company to others without the prior written consent of the Company. In the event prior written consent is granted, the Program Administrator must exercise reasonable care in the selection of any third party to which it subcontracts its responsibilities, and must ensure that each subcontractor hold and maintain proper licenses for the work to be performed and are residents in those states requiring residency and in which they render services under the Program Administrator Agreement. Notwithstanding any consent of the Company to such subcontracting, the Program Administrator retains responsibility for the performance of all services and obligations to be performed by it under the Program Administrator Agreement.

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

C. PASSWORD SECURITY AND CONFIDENTIALITY

The Program Administrator is responsible for ensuring that all passwords to on-line electronic resources (i.e. ODEN's State Rules and Regulations, ODEN Policy Terminator, AIG Policy issuance systems etc.) furnished by AIG are kept confidential and only distributed to and used by authorized staff. Access to these systems is for the sole use of Program Administrators and their immediate staff in the handling of business for AIG.

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

Appendix A

DBG INSURANCE COMPANIES

Admitted Lines

AIU Insurance Company (NY)
American Home Assurance Company (NY)
American International Pacific Insurance Company (CO)
American International South Insurance Company (PA)
Birmingham Fire Insurance Company of Pennsylvania (PA)
Commerce and Industry Insurance Company (NY)
Granite State Insurance Company (PA)
Illinois National Insurance Co. (IL)
National Union Fire Insurance Company of Louisiana (LA)
National Union Fire Insurance Company of Pittsburgh, Pa. (PA)
New Hampshire Insurance Company (PA)
The Insurance Company of the State of Pennsylvania (PA)

Non-Admitted Lines

American International Specialty Lines Insurance Company (AK)
Landmark Insurance Company (CA)
Lexington Insurance Company (DE)
Starr Excess Liability Insurance Company, Ltd. (DE)

Canada

Commerce and Industry Insurance Company of Canada (Ontario)